Universiteit
Leiden
Humanities

Just Warfare 2.0:

A Just War Theory analysis of state-sponsored cyber-attacks

Paz Maria Gonzalez-Cutre Jacobe

S2077264

Master Thesis MA International Relations

Specialization: Global Order in Historical Perspective

Thesis Supervisor: Dr. John-Harmen Valk

Word count: 14.965 words

Table of Contents

Introduction: Warfare 2.0

Due to the increase in frequency and severity of damages to national integrity and security, cyber-attacks have become a central topic to every state's agenda during the past decade. Over 670 million brand-new variations of malware were created only in 2017, an 87.7% increment over 2016 (Symantec 2018, 57); in 2017, successful breaches per business have increased from 102 cyber-attacks to 130 per year (Ponemon Institute LLC 2017, 4); 6.4 billion fake emails are sent worldwide every day (Van Kessel 2018, 5) and 1 in 13 URLs analyzed by Symantec were found to be malicious (Symantec 2018, 64). As a consequence, states have been developing cybersecurity strategies to ameliorate national security and improve the resilience of critical infrastructure and maintenance of public services. For the Fiscal Year 2019, the United States of America alone destined $15 billion to cybersecurity associated activities (The White House 2019, 273) while the European Union will invest €2 billion, for the term 2021-2027, on cyber security developments in order to boost the industry and improve the current infrastructure (European Commission 2018).

Cyberspace, usually defined as a simulated reality that associates and links computers and digital networks all around the world, has become the new battlefield for conflicts and hostile behaviors between nations and terrorist attacks (Burton 2015 and NATO 2019), meaning that there has been an exodus of conflict into cyberspace. Cyberwarfare can be described as a series of computerized actions conducted in the context of an armed conflict that entangles warlike activities that intend to target computers and technological gadgets and to control systems and networks in the virtual world. Cyber-attacks can be defined as "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (CNSS 2010, 22).

The 2005 US National Defense Strategy states that cyberspace is the new arena for military action while the Pentagon has formally accepted that cyberspace is a new battling domain, just as crucial and strategic as military activities performed on the land, sea, air and space (Lynn 2010). The Shanghai Cooperation Organization defines cyber war as “a confrontation between two or more states in the information space aimed at… undermining political, economic and social systems [or] mass psychologic [sic] brainwashing to destabilize society and state” (Gjelten 2010, 36).

Several cyber-attacks have been perpetrated by different states and organizations, aiming to affect diverse governmental entities and institutions, such as Estonia vs Russia (Traynor 2007), Israel vs Syria (Ward 2007), Georgia vs Russia (Markoff 2008), the Stuxnet worm in Iran’s nuclear program (Beaumont 2010) and Flame or sKyWIper Malware in the Middle East (Lee 2012). This is due to the fact that, generally, when there is an international armed conflict between two states, cyber-attacks will be present (Osawa 2017, 115). State-sponsored cyber-activity will seek to disorganize the correct functioning of critical infrastructure, get sensitive and classified information, interfere with military systems and convulse the democratic principles with fake information and propaganda (Osawa 2017, 115).

Cyber-attacks are not too distant from other types of attacks and can be considered as an additional means of traditional war. The intention of cyber-attacks is to provoke a certain amount of harm so that the enemy has no other choice but to follow the wishes of the attacker. Throughout history, the methods of war have been evolving, becoming more advanced and technological, but the aims of war have always been political and looking to subdue or overpower the opponent. War’s nature relies on state actors inflicting damage, destruction, injury and death for political purposes. Cyber-attacks do not change the nature of war, but provide a different means to pursue that war since they can be used to provoke and cause the same damage and harm that traditional methods do. It provides new tools that replace existing tools in order to generate the same consequences (Ricks 2014).

War is a different way of doing politics, of pursuing and achieving certain wishes and objectives. It also has an unchangeable nature and the only variation that could arise in it would be the methods of warfare, the manner in which wars are fought (Singer & Brooking 2018). Carl von Clausewitz defines war as “an act of force to compel our enemy to do our will” (Clausewitz 1976, 75) and states that “war is the continuation of politik by other means” (Clausewitz, 2007, 252). Following Clausewitz’ definition of war, cyberwar can be thus defined as the act of force intended to damage the enemy’s operating systems with the final objective of compelling them to do the will of the attacker (Schmitt 1999, 7). Wars always go after political goals (Clausewitz 2007: 28,252), have a consistent relation between tactical and political objectives (Clausewitz 2007: 74-75) and imply the use of physical fighting and destruction (Clausewitz 2007: 41, 73). Every age has its own type of war, with specific conditions and preconceptions due to distinct characteristics of players and methods, but without representing major alterations in the nature of war (Schuurman 2010, 97)**.** The methods utilized in war may change over time, but the nature of war itself will not. Cyberwar is a practice of war due to the fact that cyber-attacks act as a complement to traditional armament because they can look like kinetic violence or regular military action (Durante 2015, 369-70), and it implies the “use of cyber techniques to cause damage, destruction or casualties for political effect by states or political groups” (Lewis 2011, 23).

Just War Theory (JWT) is a limitation to the resort to war as it states which causes justify a war, the methods through which a war can be fought and the objectives that should be kept in mind when fighting a war (Rengger 2002, 354-356). The main objective of the tradition is to prevent wars and to promote peace since it offers a guideline of principles that should be followed to justify a decision of declaring war. JWT aims to limit the use of force by states, to restore peace and to pursue justice (Rengger 2013, 65).

JWT focuses on military ethics and its purpose is to prescribe a moral code of principles that will regulate the ethical reasons of war and what is permissible throughout its length of action, while offering moral principles as tools for governments to respond accurately to the situations presented in the contemporary digital battleground. However, this tradition should not be understood as a simple set of rules that stipulate what it is allowed in war, but as a political theory that expands our engagement with rights and duties in the violent sphere of world politics (Lang, O'Driscoll and Williams 2013). This means that JWT is a framework based on human dignity and that it should be used to enrich debates and augment deliberation on the just causes and the behaviour of war, with the assumption that "the burden of proof lies with those who want to wage war and who claim that their war is just" (Crawford 2003. 7). Due to the fact that nations are completely dependent on technological systems and networks for their military, social, political and business operations, the manipulation or corruption of these networks would imply a threat to national security. In this sense, the Just War tradition could offer a robust framework in guiding cyber operations and their ethical implications, in order to establish a determined set of values that could educate leaders, states and policy makers on how to act in the case of a virtual conflict.

JWT has in itself different ethical theories that provide several ways of interpreting its principles and application to reality (Bellamy 2006, 229). For the purpose of this thesis, a Classical conception of the tradition will be followed on the basis that the modern reworking of the just war and its concept of 'legitimate force' is considered to be more permissive than it should be, acting as a driver or a facilitator on the use of force by states (Rengger 2013). The Just War tradition was developed during the Middle Ages with the aim of limiting the resort to war and that, in the case that it is absolutely necessary to declare war, it should have as main objectives the pursuit of peace, the restoration of justice and the punishment of a wrongdoing. Modern Just War theorists understand this theory as a way to validate or invalidate wars, focusing on the legitimacy of force instead of evaluating the concept of use of force itself and its implications. They build their arguments by associating the punishment of wrongdoing with the promotion of justice that eventually leads to a more permissive attitude on the use of force (Rengger 2013). This means that Modern theorists do not seek to limit the resort to war, but instead to validate the decision of going to war by misinterpreting the different principles and expanding their meaning. These concepts will be further developed and analyzed in chapter 1.

This thesis will study two cyber-attacks under the light of JWT principles in order to contemplate and understand the morality of those attacks and to reflect if new principles should be developed in order to respond to the challenges of the particular nature of cyberspace. The final purpose of this study is to answer the following question: *“To what extent can Classical Just War Theory principles offer a moral guidance on state-sponsored cyber-attacks?”*.

By answering this question, it will become apparent that Classical JWT correctly addresses the moral queries on cyber-attacks. JWT offers accurate answers to the ethical issues that conventional warfare presents due to the fact that some cyber-attacks can provoke serious physical destructiveness that is comparable to conventional attacks (Finlay 2018, 358) and that can amount to constitute a type of armed conflict and to assist and strengthen the conduction of war in a traditional way (Durante 2015, 369-70. As a consequence, JWT should be considered the ethical framework that guides cyber-attacks.

To support this claim and through an extensive study of the factual evidence of each case under the light of JWT principles, this work evaluates two cyber-attacks that were allegedly sponsored by states and that were aimed to harm or destroy civilian infrastructure: Stuxnet and Black-Energy-Industroyer, through an extensive study of the factual evidence of each case under the light of JWT principles. This thesis argues that JWT focuses mainly on the effects and intentions that an attack has, rather than the means used, and that a nation that suffered an unjust attack will be able to vindicate itself and punish a wrongdoing if there is an ethical analysis of the situation by following JWT principles (Cook 2010, 416).

The two case studies have been selected due to the fact that they have been the first cyber-attacks that provoked effects in the real world and that they were, allegedly, sponsored or pursued by nation-states to attack other nation-states. This specific selection was based on the premise that war is a specific practice that implies public violence “on behalf of and mandated by the state toward another similarly constituted entity” (Reitberger 2013, 69). Stuxnet has been described as the most sophisticated piece of malware ever designed: its refined code moves a step further from preceding attacks of analogous nature because it provoked damages in the real world to a clearly defined target (Halliday 2010). BlackEnergy-Industroyer are two cyber-attacks that were aimed at the Ukrainian power grid within the geopolitical military conflict between Russia and Ukraine. They are relevant because they were the first two successful cyber-attacks against a power grid and have been the first cyber warfare attack to disturb civilians due to the fact that they provoked extensive power blackouts for several hours (Cherepanov & Lipovsky 2016 and Khan et al 2016).

This thesis comprises three chapters that will explore the Just War Tradition and its relation to state-sponsored cyber-attacks. The first chapter will set out the JWT framework by revising current debates on the tradition, it will establish the fundamental concepts of the tradition and it will argue that the tradition determines which conditions morally justify war and what actions should be followed during the course of the war. The second chapter will develop the facts of the Stuxnet case under the light of the Just War Principles and will consider that Stuxnet was a morally unjust cyber-attack because the attackers failed to comply with most of the JWT principles. The third chapter will expand on the BlackEnergy and Industroyer cyber-attacks by analyzing the historical and political context of the Russo-Ukrainian war and will argue that they were both morally unjust because the attacker had no just cause to attack and as a consequence, all other principles cannot be complied with due to the lack of just cause. Lastly, a final conclusion and reasoning will be presented based on the fact that, although there should be a deeper study on the arising issue of attribution, JWT offers a proper moral guidance to politicians and state leaders when discussing the morality of cyber-attacks due to the fact that JWT does not study the weapon chosen to pursue an attack, but the attack itself.

Chapter 1: The Just War Tradition

The Just War tradition is a restraint to the resort to war: what we can rightfully fight for and the ways in which we can rightfully fight with the aim of restoring justice and peace (Rengger 2002, 354-356). This means that the tradition states what the conditions are to morally justify the decision to go to war and what actions can or cannot be followed during the course of the war (Primoratz, 222). It is a theory that looks to limit destructiveness, restore peace and punish a misconduct (Rengger 2013, 65).

Just war thinking indicates that war can be, on certain occasions, an instrument of justice that can help put right to an immense injustice or that can restore order where there is lack of (Elshtain 2003, 50). During war, states should remain honorable at all times and the punishment should start with reason and not with malice, based on the fact that wars should be waged with the aim of pursuing justice and peace and not self-gain or revenge (Cicero 1991, 18-38). Furthermore, wars should be defensive and punitive since offensive and preventive wars are forbidden because no harm would be inflicted before declaring war. In order to administer a just punishment to wrongdoers, men should refrain from the enjoyment in the sufferings of others, avoiding returning evil for evil: wars should not be fought out of feeling of revenge, anger or hurt (Lee 2012, 43). Thus, undergoing enjoyment while punishing or having just vengeance is an injustice per se (Mattox 2018, 19).

There are certain criteria that should be met in order for a war to be considered just: these criteria seek to promote justice, restore peace and the fundamental aim to right wrongs as a mean to restore the *status quo ante bellum*, but also to punish the wrongdoer (Russell 1975, 19). They also limit the resort to war because war should always be the last resort and, before declaring it, all other preventive measures should have been exhausted (Oliphant 2007, 139).

The principles of JWT can be divided into two categories: *jus ad bellum,* which consider the moral justifications of going to war by addressing specific conditions that should be fulfilled so that the resort to war is morally substantiated; and *jus in bello*, which include the moral permissibility of the conducts that should be followed while fighting a war by acting accordingly to ethical principles that rule personal or collective conducts in war (Parry 2015, 176). It is important to follow the totality of principles because they are the restraint standards that should be considered as the necessary conditions to go to war (Childress 1986, 269), and they allow an analysis on the real need to the resort to war. Also, in the case that extreme violence was deemed necessary, they limit both the military conduct and the just combatant's behaviour (Cox 2014, 24). In this sense, wars should only be fought if peaceful means are not available or effective, and the best way to end a war is to achieve a just peace, thus a limitation to the use of force should be pursued (Lee 2012, 41).

Classical Just War thinking was developed within a group of premises that define a good government and are articulated as the three objectives of politics: order, justice and peace, which in turn were considered to be interconnected and dependent on each other. The conditions for a just war that serves the aforementioned objectives correspond to: "the necessary authority to the end of order, the requirement of just cause to the end of justice, the requirement of right intention to the end of peace" (Johnson 2013, 41). Moreover, Classical JWT reinforces the thought that war is an extreme realm, emphasizes that the principles are a restraint to both the use of force and focusses on both the ideas of punishment of a wrongdoing and pursuit of peace and justice (Rengger 2013, 65). In this sense, the Just War principles should not be interpreted as part of a checklist to declare war, but instead as a guidance to limit the resort to war and to use it as a last resort at all times, looking for alternatives that might offer a better solution. It is important for military and political leaders to understand and reflect on the moral fundaments of deciding to wage a war and to distinguish the way wars should be conducted (Rengger 2002, 355).

Modern JWT, on the other hand, appears to be problematic because it does not illustrate the peace-making imperative that corresponds to the main aims of Just War as Classical JWT does (Kunkel 1983, 506). It also treats the *jus ad bellum* and *jus in bello* as two separate and independent categories, with a growing pre-eminence of the latter. There is a bigger influence on what the rights of states are, especially the right to use force in order to defend its interests, while the *jus ad bellum* principles are considered superfluous (Rengger 2013, 66). This implies that there is a flourishing priority on the eradication of wrongdoing through the use of force over the limitation on the resort to war, resulting in a less restrictive JWT in relation to the causes and the use of force. In this sense, there is a distinction between the *jus ad bellum* and the *jus in bello* principles and the two categories are considered to be incoherent with one another and should be judged independently (Walzer 2006, 21). As a consequence, the relationship between justice and war will be different in these two categories since the justice of a war in one of them does not necessarily imply a connection to the justice of the other (Parsons 2012, 664). This means that one can wage a just war in an unjust manner, consistent with the *jus ad bellum* criteria but in violation of the *jus in bello;* and one can wage an unjust war in a just way, with a violation of the *jus ad bellum* but consistent with the *jus in bello* principles (Walzer 2006, 21).

The Just War Theory Principles

Two main categories differentiate the Just War principles: *jus ad bellum* (criteria that determine the permissibility of engaging in war) and *jus in bello* (criteria that establishes the conducts to be followed during the war). Just War principles are restraint standards that reflect on the moral objectives of waging a war and permit an in-depth analysis of the situations in which the resort to war is considered necessary. In case that a nation fails to fulfil all the criteria, the war will be unjust.

For the *jus ad bellum* or the resort for war to be morally justified, the following principles should be met: just cause; right intention in going to war; public declaration of war by a legitimate authority; reasonable hope of success to prevail; proportionality and last resort.

Regarding the *jus in bello,* the discussion focuses on two requirements that should be satisfied in order for an act to be morally permissible during war: discrimination and proportionality (Parry 2015, 177). Proportionality implies that the damage inflicted on the enemy is worth it and corresponding and equitable to the one received, weighing the evils and goods from violence in terms of effectiveness and value (O'Brien 1982, 21). Discrimination means that there should be a clear differentiation between combatants and non-combatants.

The selected criteria appear frequently in extensive just war theories. Such list has been constructed from the works of Johnson (1999, pp. 28-29), Hartle (2004, pp. 96-97), Hurka (2005, pp. 35-36), Frowe (2011, pp. 52-72), and Orend (2005, sections 2.1 and 2.2).

1- Just cause

A just cause functions as a restriction on the type of ends or aims that might justly be pursued or achieved through war. Only specific types of ends provide a moral argument for killing other human beings (McMahan 2005, 4). Classical JWT states that the just cause should be based on three premises: i) the right to defend one self, ii) the right to recover lost property, and iii) the right to vindicate suffering and penalize a wrongdoing (Cicero 1991*,* 11-13). The right of self-defense is limited in the sense that the use of force is the only way to prevent an attack that has already commenced or that is inevitable. If the attack is thought to be potential, then other means should be utilized (Grotius in Whewell 1853, 63-65). According to this line of thinking, a preventive war is not an accepted just cause, since a just cause necessitates a wrongdoing, and in a preventive war no harm has been received and no actual aggression occurs, therefore no just cause exists. It is unacceptable that a person should be punished for a crime that he has yet to commit (Vitoria in Padgen & Lawrance 2001, 316).

Modern Just War theorists consider that preventive wars are just causes to go to war due to the fact that any person who threatens another individual with imminent damage is liable to be killed. A universal application of this theory would be extremely lenient to violently resist any attempt to force, since simply posing a threat of harm or attack would be a sufficient cause to establish liability to counter-attack (Barry 2011, 459). If any use of force or imminent threat made by a state is considered an aggression to the rights of another state, that implies a threat to the security of that state, then a state can be considered an aggressor only by threatening, regardless of the existence of its intention to launch a first strike. In this way, just war stopped being a restraint or limitation to the use of force to be a justification and legitimization of the resort to war: the principle of just cause only applies to the initial resort to armed conflict, and after the commencement of war, the only important thing is how war is operated. Since just cause is a mandatory element to engage in war, it should be taken into consideration before and during war because it specifies the ends through which is it admissible to engage in war and it determines the conditions for the end of the war (McMahan 2005, 2).

The absence of a just cause has strong negative effects on the severity of the proportionality principle because, when there is no just cause, all the individuals targeted during the war are innocent, and the injuries provoked over the innocent weigh more against the objectives of a war than the injuries provoked on those who are liable for wrongs made to others (McMahan 2005, 15). A just war is one that seeks the restoration of peace and justice and the punishment of a wrongdoing, thus in the absence of harm, warfare is not justified. It is morally unjust to punish or cause injury to those who have not caused any harm (de Vitoria in Pagden & Lawrance 1991, 304).

There is an essential element that should be present in order to study the just cause: the attribution of the aggression. The identity of the attacker should be known in order to respond in a just manner, meaning that the act of self-defense should be aimed at the correct aggressor and a misattribution would signify a wrong prosecution of the incorrect parties for a conduct they did not commit, while at the same time giving those parties a just cause to respond (Dipert 2010, 401).

Around the just cause rely the rest of the principles, because the just cause conveys the ends for which waging a war would be justified and, when the just cause has been achieved, then the war should end because without a present just cause there would be no justification for it (McMahan 2005, 1). Also, the right intention and the proportionality principle will be defined in relation to the just cause, therefore the just cause is essential for the pursuit of a just war.

2- Right intention

The right intention means that war should be waged with the ultimate goal of peace in mind and should not to seek for revenge or territorial expansion. It has a subjective character and has a predisposal to satisfy only legitimate objectives. The right intention principle "aims to overcome the possibility that a state may have a just cause, but still act from a wrong intention" (Koeman 2007, 201). Wrong intentions have in mind acts or results that do not serve to substantiate a state's just cause (Burkhardt 2017, 9). Wars that are waged with impure motives such as "love of violence, revengeful cruelty, fierce and implacable enmity, wild resistance, and the lust of power, and such like" (Augustine 1887, 301) render the war unjust because they are clearly not related to restoring justice (Johnson 2001, 29). Therefore, the right intention should include both the prevention of wrong intentions and the positive objective of securing peace (Johnson 2005, 8). Without a right intention, "the connection between one's actions and the reason that justified it remains contingent, and this allows for the possibility that just cause could be only a pretext or excuse for bellicose action aimed at some further goal beyond that which one's justifying reason supports" (Boyle 1996, 45).

During war, right intentions are related to the search for peace and conciliation, refraining from causing unnecessary harm, destruction or imposing illogical conditions (U.S. Catholic Bishops 1992, 100). Therefore, an examination of the motives of going to war is necessary because war should conduce to a just and lasting peace. In this way, "our actions in war should cohere with our stated aims in going to war…if a belligerent's acts in war do not appear to cohere with that belligerent's stated intentions, then we have a good reason for assuming the belligerent was advancing false aims for the war" (Cole 189).

3- Competent authority

Competent authority is the sufficient authority to declare war, which establishes a difference between the wars that were held looking for the common good and those that were private. This requirement also states who is able to judge if a war is just, if it has a right cause or if it would have a proportionate comeback, as well as who is enabled to act based on that evaluation (Fabre 2008, 963). The sovereign has an obligation, a duty, to wage war against an enemy that is evil and unrighteous (Augustine in Dyson 1998, 929). The political community's safety and protection is entrusted to the authority, and the joint activity of engaging in war and the mobilization of forces can only be achieved by a first agent who has been appointed for this matter (Reichberg 2012, 352-353). The concept of competent authority is construed on the logic that "war is a collective enterprise of the highest political community, the polity (respublica)" (Reichberg 2012, 359), the republic, and only those who are leaders of the community can wage war in the name of the community.

The authority principle is essential for two main issues: the first one entails the evaluation of the claim to have a right to commence war, and the second one involves an analysis on what is morally allowed within war (Finlay, Parry and Wrange 2017, 168). It is the principle that focuses on answering who can start a war and direct its pursuit (Toner 2010). The resort to war should be made by a state, through the pertinent procedures that allow the legal authority to raise the armed forces against the enemy (Fotion 2007, 18-20).

However, Modern theory rejects the principle of right authority on the basis that territorial integrity and political sovereignty are considered the agglomeration of particular and personal goods, so "there is no communal values as such; they are only precious as an extension of the rights of individuals" (Braun 2018, 231). As a consequence, the resort to war would be less limited in the sense that any individual could declare war because they must defend their goods and rights. This idea results problematic because the requirement of competent authority is utilized to limit the resort to war as rationally as possible (Braun 2018, 233), and granting any type of individual the possibility of having the authority to declare war would mean complete chaos (Coates 2016, 156). In this sense, the competent authority principle works as a limitation on private uses of armed force and discarding it will most certainly prompt an increase in violence (Braun 2018, 233).

4- Reasonable hope of success

Reasonable hope of success establishes the need to not use force unless there are reasonable possibilities of achieving our objectives or win the war. The main argument of this principle is that war has varied costs and unless there is an opportunity to win the war, the cost of going to war for the sake of it is too high. Therefore, an analysis of the potential costs and benefits of waging a war should be made in order to establish if there is high certainty of a probable success (Harbour, 232). This could be done in a numerical way by evaluating the probable set of costs and benefits that might occur by making a determinate decision, and then make a comparison with other results from other decisions (Harbour, 232). As a consequence, the reasonable hope of success establishes the amount of force to be employed and "if none of the just and serious ends…could be realized, or fulfilled through the war, a nation should reconsider its policy" (Childress 1986, 264).

5- Proportionality

Proportionality has a double function: proportionality in the war itself (*jus ad bellum)* and proportionality in the means employed (*jus in bello)*. The proportionality in war means analyzing if the just cause is sufficient to compensate for the damages that the war would cause, both human and material. Based on this, a war can be considered unjust when there is a just cause, but the costs of the war are bigger than the benefits. War should be a proportional answer to the events that establish a just cause. This is due to the fact that "it is not every cause that is sufficient to justify war, but only those causes which are serious and commensurate with the losses that the war would occasion" (Suarez 1944, 816). The main idea of this concept is to ensure that when both sides of the war incur in imminent damages and destruction that result from the conflict, these are justified due to the gravity and relevance of the cause (Brown 2003, 175). On the other side, proportionality of the means imposes limits to the actions that can be undertaken in war and demands a differentiation of combatants and non-combatants (Carmola 2005, 95-96). The military operations should be proportionate to the aims of the war, and thus limited, because the force used should not be excessive and the harm imposed should be limited (Lebow and Stein 1994, 129).

Proportionality implies that the relevant negative consequences attributable to war cannot be out of balance to the relevant good effects (Hurka 2005, 40). There is an implicit obligation to anticipate that greater damages do not arise from the war than those that the war would avert (Vitoria in Padgen & Lawrance 2001, 315), since the main idea is that the damage of war should not be excessive to the damage the war would avoid. The fundamental cost that needs to be taken into consideration is the human loss that every attack cause, thus the force can only be used against a legitimate military objective (Fotion 2007, 21).

Modern theorists state that "proportionality plays only a marginal and uncertain role" since there is no clear way of measuring the benefits and damages in numerical values that the destruction of war might entail (Walzer 2015, 129). This line of thought provides a more permissive way of waging wars and distorts the notion of just war out of proportion (Carr & Kinsella 2013, 27-29), due to the fact that without the principle of proportionality everything would be permitted in order to secure victory.

Classical thinking, on the contrary, understands that in order to determine the proportionality principle, three elements have to be taken into consideration: i) analysis of the benefits of the war, ii) evaluation of the costs of the war, and iii), how these two can be measure or scaled against each other.

(Hurka 2005, 38). In this sense, it would be unjust to cause a higher amount of harm by defending against an aggression than the injuries that the attack would create.

6- Discrimination

The principle of discrimination entails a differentiation between combatants and non-combatants during war and that attacks should be directed towards military objectives while trying to preserve the safety and security of the civilian population (French, 152). In this sense, during war, the only objectives should be enemy combatants, and non-combatants should never be direct targets. However, the latter are not immune from total harm since there may be attacks in which they are not the objective targets but are part of the collateral damage of a legitimate attack to a military target (Coleman, 2013, 151).

The criterion of discrimination holds that "combatants must discriminate between those who are morally responsible for an unjust threat, or for a grievance that provides a just cause, and those who are not" (McMahan 2004, 722-723). It is formulated in the sense of who can and cannot be attacked by the armed forces in their search for military objectives (Toner, 2010 96), differentiating those that can be attacked deliberately and those that should be seen as immune (Finlay 2012).

Authors like Paul Ramsey and Michael Walzer, Modern Just War theorists, put great emphasis on the *jus in bello* principle of discrimination because it states the ways a war can be fought and its implications (Johnson 2002, 138). A war can never be considered just if the discrimination principle is not followed, but this line of thought is questionable because it gives secondary importance to the *jus ad bellum* principles. The *jus ad bellum* criteria are a limitation to the resort to war, while the *jus in bello* principles express what can and cannot be done while waging a war. If *jus ad bellum* principles are discarded or have an inferior relevance, JWT would therefore not be a guideline to understand the circumstances in which war should be waged, but a theory that focuses on what is permitted to do in war (Rengger 2002, 354-356).

7- Last resort

The principle of last resort is a consequence of the will to limit the resort to war, and it establishes that all alternative solutions must have been exhausted. This means that resorting to war is allowed if and only if all other peaceful options that had a reasonable chance of success of reaching a just aim have been undertaken for a reasonable period of time and have failed. The justification of this principle relies on the fact that war results in the deaths of innocent people and in the massive destruction of property, therefore it should be avoided when possible (Aloyo 2015). Moreover, the harms inflicted by war itself should not superior than the harms received by the unjust opponent, thus avoiding unnecessary destruction and death (Yoder 2001, 2). If the costs of the war are higher than the costs of the political community in whose name the war is being fought, then the war cannot be justified in the moral sphere.

A more permissive view is the one provided by Modern JWT: the theorist Michael Walzer expressed the last resort should be discarded because if taken literally, "the 'last resort' would make war morally impossible. For we can never reach lastness, or we can never know that we have reached it. There is always something else to do: another diplomatic note, another United Nations resolution, another meeting" (Walzer 2004, 88), thus war could never be achieved. In this view, diplomacy would play no role and war could be declared at any time. However, if the just cause can be accomplished by less destructive mechanisms like diplomacy, then entering into active combat is immoral (Hurka 2005, 35).

The last resort principle considers that war should always be the last achievable and attainable option, but the relatively best non-violent viable and reasonable option(s) must be tested first (Pattinson 2015, 952). The principle should not be considered as an absolute prohibition of the resort to war, but as a limitation to war that implies going to war when all other options have been exhausted (Pattinson 2015, 952-953).

JWT discusses the ethics of war and states the criteria that should be met in order to consider an armed conflict to be morally justified. Classical JWT offers a clear and coherent guideline that reinforces the concept that war is an extreme domain and that the principles should be understood as a limitation to the use of military force while aiming to pursue peace and justice (Rengger 2013, 65). On the contrary, Modern JWT has a more permissive interpretation of the principles that are contrary to the peace-making imperative that coincides with the Classical viewpoint of the theory, giving more importance to the *jus in bello* than the *jus ad bellum*. The Modern viewpoint separates and judges independently the two categories of principles and is more focussed on the means and ways of waging a war rather than a restricting the use of force. However, all the principles should be considered as a whole and they cannot be discarded, since their main aim is to limit the resort to war and to seek for other alternatives that can offer a more peaceful solution to a conflict.

Due to the fact that cyber-attacks have been evolving and becoming more frequent, it is necessary to establish certain principles that will guide states in their pursuit for justice and peace. In the following chapters, two case studies will be analyzed under the light of Classical JWT in order to establish if these principles are applicable to the new computerized threats or if they should be updated to respond to a type of attack that, due to its particular characteristics, should be in a different category in war ethics.

Chapter 2: Stuxnet

JWT is a guideline that acts as a limitation to the resort to war and has as main aim the pursuit of peace and justice. The theory twirls around seven principles that should be satisfied in order to go to wage a just war: just cause, right intention, competent authority, high probability of success, proportionality, discrimination and last resort. Classical JWT emphasizes the fundamental concept of peace-making and enhances the necessity to follow all the principles so that, in the case that all non-violent alternative solutions have been exhausted, war ends up being an extreme realm and the last resort. All the principles should be considered as a whole and they cannot be discarded, since their main aim is to limit the resort to war and to seek for other alternatives that can offer a more peaceful solution to a conflict. This is due to the fact that *jus ad bellum* principles work as constraints on the initiation of war in order to avoid unnecessary battling and the *jus in bello* criteria function as a restriction to the ways wars can be fought so as to dissuade the utilization of weapons or strategies that might cause avoidable and unneeded harm to the enemy (Schulzke 2017, 1). In this sense, Classical JWT offers a comprehensive instruction to state leaders and policy makers in regards to cyber-attacks, due to the fact that they are an act of force that intends to damage the enemy's operating system (Schmitt 1999, 7) and always go after political goals (Clausewitz 2007, 28). Although the methods and weaponry utilized in war may change, the nature of war remains the same.

This chapter will describe the key events of the Stuxnet cyber-attack, focusing on the political context and the specifications of the attack itself and will revise them through the consideration of the *jus ad bellum* and the *jus in bello* principles. In this sense, under the light of the tradition, Stuxnet should be considered a morally unjust cyber-attack against Iran's nuclear facility due to the fact that the attackers failed to comply with the principles of just cause, proportionality, competent authority, right intention, and discrimination. The attackers did adhere to the criteria of last resort and reasonable hope of success: the success in destroying the centrifuges and delaying Iran's nuclear programme for several years indicates that the aggressors had a vast knowledge on how to accomplish their aims and were certain that they would prevail. Despite the fact that the attack was anonymous, there are reliable sources that the USA and Israel were behind it: several members of the Situation Room meetings of Project Olympic and officials of the US government have stated that President Barack Obama ordered the sabotage of Iran's nuclear facilities (Sanger 2012). Moreover, General James Cartwright, former Vice Chairman of the Joint Chiefs of Staff, pleaded guilty on sharing classified information related to the Stuxnet virus to journalist David Sanger (Groll 2016). This implies that the White House was aware of the existence and development of Stuxnet and of the use that it would have. Thus, although the USA and Israel did not claim the authorship of Stuxnet, there are certain facts that indicate that they were behind it.

Stuxnet is a sophisticated technological weapon built and engineered to be utilized in one of the most critical current political issues: the Iranian nuclear proliferation (Fidler 2011, 57). Its main aim was to delay the development of Iran's nuclear programme and to avoid the proper operations and functions of its facilities (IISS 2011, 2). Stuxnet is a relevant case for the study of ethics of cyber warfare because it is the first weapon to overcome the gap between mere cyber-activity to physical destruction in the real world (Jenkins 2013, 69). Previous cyber-attacks remained in the digital sphere and they implicated activities such as fraud, piracy, manipulation or exploitation of information, but caused no physical consequences (Singer & Friedman 2014, 68). Stuxnet broke down machinery by creating an explosion, resulting in a new type of threat to a state's critical infrastructure: a weapon made of bits that provoked physical damage (Singer 2015, 83).

The Stuxnet attack was part of a broader campaign code-named "Olympic Games", allegedly an US-Israel collective operation against Iran (Lindsay 2013, 366). Mahmoud Ahmadinejad won the 2005 presidential election, solidified conservatism in Iran, restarted Iran's nuclear activities and increased tensions with both the United States and Israel (MacAskill & McGreal 2005). Allegations of illegal and clandestine nuclear weapons development were made against Iran and an investigation established the presence of non-compliant issues in Iran's nuclear activity (Kerr 2015, 4) and the fact that they tried several non-violent alternatives means that the attack as a last resort. The United Nations Security Council ordered Iran to stop its uranium enrichment and reprocessing and to follow additional security measures. However, Iran indicated that its nuclear production was solely intended for peaceful and non-military activities (Nakashima & Warrick 2012). Consequently, the intelligence agencies of the United States and Israel allegedly initiated a collaborative effort to sabotage Iran's nuclear production, delay its nuclear program and secure their position in the Middle East (Sanger 2012).

All nation-states have a just cause to defend and protect their inhabitants and their territorial domain from an external attack (Regan 2013, 48), but in the case of Stuxnet, the United States and Israel did not have a just cause to attack Iran's nuclear facility due to the fact that Iran stated in several occasions that the centrifuges were intended for peaceful non-military economic activities and it has denied the possession of a nuclear weapons programme (Bowen & Kid 2004). Iran had greatly developed its uranium enrichment by making use of centrifuge technology produced in Pakistan, and although lightly enriched uranium (LEU) is suitable for peaceful nuclear power, the same centrifuge system could be operated in the production of highly enriched fissile material (HEU) (IAEA 2010). As a consequence, Israel stated in several occasions its opposition to the nuclear developments in Iran, and there has been speculation around the actions that Israel could take in order to impede Iran's progress in its nuclear program (Mahnaimi & Baxter 2005, Bruce 2006, Federman 2006). The United States rejected the possibility of a kinetic attack, first because a counter attack by Iran would have been catastrophic and second due to the public opinion of unaccepted U.S. participation in the Iraq and Pakistan war. The US had lost power, popularity and credibility in the Middle East area due to its failure in the Iraq and Afghanistan wars and to the lack of ability of the Arab governments to follow Washington's orders. It had also failed to push Iran's nuclear ambitions backwards or to implement the United States' policies (Babaei 2008). On the other hand, Israel was concerned with Iran's foreign policy and its aggressive approach after 9/11: the turning point was when a truck was captured by Israeli troops transporting a consignment of weapons and explosives from Iran to Palestine (Gasiorowski 2007). On the other hand, Iran could solidify its position due to the defeat of its eternal Arab rival, Iraq, and to the rise of a pro-Iranian Shiite command there. Moreover, tensions increased because Iran had been constantly providing weaponry to Hezbollah, which made Israel develop its military capacity and maintain its superiority over the other states of the region. As a consequence, The United States and Israel saw the development of Iran's nuclear facilities as a threat to international security, and allegedly used Stuxnet as a preventive attack that aimed to delay Iran's nuclear programme for a long period. The nuclear program itself cannot be considered a threat for the international community, but since Iran is a signatory of the Nuclear Non-Proliferation Treaty it should have followed its rules. In this sense, the International Atomic Energy Agency (IAEA) could not rule out the existence of a nuclear weapons program in Iran.

The United Stated and Israel allegedly executed a preventive attack against Iran's nuclear facilities with the objective of interrupting Iran's nuclear development and to ensure that it would not develop any nuclear weapons while using self-defense as a premise. Prevention implies to aggress the opponent when an attack is plausible or imminent, and as such the choice of resorting to war has been made by the enemy (Gray 2007, v). However, according to Classical JWT, a preventive attack is not a just cause for war because one cannot punish someone for something that they have not committed yet, thus attacking Iran's nuclear facilities based on the assumption that these might be used for uranium enrichment for nuclear weapons does not fulfil the just cause for war. Expanding the concept of self-defense while incorporating the idea of preventive attack proves to be problematic due to the speculation and uncertainty of acting on threats before they actually materialize into action (Fiala 2008, 79). In this sense, a harm cannot be resisted before it has been inflicted (Reichberg 2007, 7). In the United States, there are two doctrines that relate to preventive war and that have marked the way that the United States defines a legitimate threat. First, the 1841 Webster Doctrine that defines a legitimate defense as the one that responds to threats that are "instant, overwhelming, leaving no choice of means, and no moment for deliberation" (Reichberg et al 2006, 563-64). Second, the Bush Doctrine which claims that the United States' use of military force would be legitimized and valid when employed to "prevent or forestall hostile acts by adversaries… even if uncertainty remains as to the time and place of the enemy's attack" (The White House 2002, 15). These ideas advocate for a doctrine of authentic and plain prevention capacity, which is inconsistent with the basic principle of just cause that an offensive war should be waged only when it is a response to a previously inflicted wrongdoing (Reichberg 2007, 33).

The use of Stuxnet implied an economical damage and the destruction of physical property and, as a consequence, the United States and Israel have given Iran a just cause to counter attack. The malware worm was created in order to target facilities that use a special kind of Siemens software that was employed in the control systems of Iran's nuclear facilities, propagating as extensively as possible. Through the laptops and memory sticks of different Iranian scientists, the worm penetrated the security system of the nuclear facility (Singer 2015, 81). Once it got in contact with the target system, it was set to automatically attack it by infecting the Siemens software in the facility's control systems and the one's of the frequency converters that were supplied by two companies: Vacon and Fararo Paya (IISS 2011, 1). The attack did not stop the functioning of the centrifuges but instead it provoked changes in the pressure inside the centrifuges and modified their speed, by slowing them down, then returning them to their normal speed and finally accelerating them beyond their maximum limit. In this way, the centrifuges could not produce refined uranium and eventually broke down or exploded (Singer 2015, 82). JWT states that self-defense from an attack and the destruction of property are just causes for war, and as a consequence of the Stuxnet attack, Iran would have just cause to respond in the kind and to punish a wrongdoing by utilizing malware that would impose a comparable economic amount of loss to the United States and Israel (Eberle 2013, 59).

The harm made to the centrifuges is quantifiable and identifiable: 1000 centrifuges were damaged and the nuclear program was delayed for several years, causing a massive economic loss for Iran. Since the United States and Israel did not have a just cause to carry on the attack there is no possibility to establish the proportionality principle, but Iran does have a just cause to counter-attack and employ certain means that are proportional to the evils suffered. In order to apply the proportionality principle three things need to be identified: the benefits, the costs and the weight of one against the other (Hurka 2005, 38). This is done with the aim of analyzing if a war can be just in spite of all the suffering, killing and destruction caused (Forge 2009,36). An issue that might appear in cyberattacks is that of measuring the amount of harm received because it could jeopardize a possible counter-attack due to its disproportionate retaliation (Lin, Allhoff & Rowe 2012, 25-26). When a contemplating proportionality on cyber-attacks, damage is difficult to assess due to the lack of knowledge of the computer systems implicated and of the connections that those systems might have with other systems (Richardson 2011, 25). However, Stuxnet was an attack that, unlike other cyber-attacks, caused physical destruction in the real world and, as a consequence, the damage inflicted could be counted and measured.

There was no official declaration of war from the United States and Israel against Iran, therefore the Stuxnet attack fails to satisfy with the competent authority principle. The legitimate authority principle is restricted to special entities that have specific characteristics: they are sovereign and represent a political community (Reitberger 2013, 65). The United States Constitution in its Article 1, Section 8, establishes that the Congress is the institution entrusted with the capacity of declaring war. In the case of Israel, Article 40 of the Basic Law of Israel Defense Forces states that the government must make a declaration of war and that this act should be taken to the Parliament for approval. The competent authority, being an individual or state's body, "must be a duly constituted authority widely recognized as having the right to wage war. This generally refers to the representative of a sovereign political entity; states, today" (Johnson 2005, 38). The source of legitimacy to declare and fight a war derives from sovereignty or from a widely acknowledged authority (Reitberger 2013). In this way, the resort to war is limited to specific that have developed approval procedures and that are authorized to do so. The just war requirement of competent authority establishes who can determine if a war is just, whether there is a just cause, what proportionate response it would entail, who can act based on that reasoning (Fabre 2008, 963) and it gives the right to go to war to sovereign political organizations that implement laws within a specific territory (Fabre 2008, 964). If this principle is discarded as Modern JWT suggests, the chances of fighting a war for the just reasons will be worsen because it is the competent authority who judges the justness of a war and who evaluates if there is a just cause and if the counter-attack is proportionate (Fabre 2008, 963). Fighting a war without following the competent authority principle would mean that there would be no difference between an attack from a state or a terrorist group or mere banditry, and with no clear chain of command wars will not be fought with just means. On Stuxnet, there has not been a claim on the authorship of the attack but the time invested in the code, its unprecedented characteristics and the resources needed to develop it clearly indicate that it was state-sponsored (Fidler 2011, 57). Stuxnet manipulated two stolen digital certificates of authenticity of two enterprises to cover its malicious code and appear to be legitimate; exploited four zero-day security vulnerabilities in Windows systems and targeted the programmable logic controllers (PLCs) that operated on industrial control systems adhered to Iranian centrifuges operating in enriching uranium. Moreover, it altered PLC software to make the centrifuges start spinning at high speeds that would cause damages on them and disguised the modified speeds from the verification systems by way of code that registered and reiterated information displaying normal performing conditions. The virus was dispersed in three different versions before being detected and spread through varied methods, that included removable hard drives, Microsoft Windows zero-day vulnerabilities and the Internet, provoking the damage of approximately 1.000 centrifuges and developed specific characteristics to reduce to a minimum collateral damage and to finalize the worm’s activeness on a definitive date (Falliere, Murchu et al 2011).

The high-level design of Stuxnet shows that its creators knew exactly what they were doing and the ways to target their objectives, they clearly analysed and studied the ways to perpetrate their attack to the Iranian nuclear facilities that resulted in a secret cyber-attack that was discovered a long time after its arrival to the Natanz nuclear facility, therefore the attackers had a reasonable hope of succeeding. This principle involves the analysis of the possibilities that a state has to triumph within a war, whose purpose is to prevent absurd or pointless fighting when the results will be clearly excessive or unreasonable (US Catholic Bishops in Elshtain, 100-101). If a state resorts to war but has no chance of prevailing, it is being reckless (Childress 1986, 264) since a reasonable chance of success means "successfully using force as a means to other morally defensible values" (Harbour 2011, 234). In order to see if an actual military victory could be achieved. The clearest example of the application of this principle would be the prudent decision of Czechoslovakia to not fight a war against Germany in 1938, since war would have costed too much and achieved almost nothing (Harbour 2011, 235). The moral implications of this decision had to do with answering whether the purposes of the war can be accomplished and is closely connected with the proportionality principle: waging a war where there is a low chance of prevailing implied causing harm in a disproportionate way (Harbour 2011, 236): civilians and soldiers are killed, property is destroyed, and physical and psychological damage is inflicted to different people. Thus, the reasonable hope of success means bringing to a successful conclusion the just cause, prevailing in the military sphere, because if the hope of success can be achieved without resorting to war, then other alternatives should be used before war, leaving war as a last resort (Eckert 2014, 64).

In the Stuxnet cyber-attack there is an absence of a just cause and therefore an absence of right intention. This is due to the fact that the right intention is rationally linked to the just cause and the right intention will only be satisfied if a war is waged for the just cause (Coady 2008, 98-99 and O'Brien 1981, 34). It can be difficult to assess the real intentions that Israel and the United States had in mind when deciding to attack Iran. In a way, the right intention to attack Iran's nuclear program could be related to the 2002 public speech of President Ahmadinejad, who stated “there is no doubt that the new wave [of attacks] in Palestine will wipe off this stigma [Israel] from the face of the Islamic world. As the imam said, Israel must be wiped off the map” (Ahmadinejad in MacAskill & McGreal 2005). In this sense, the preservation of Israel’s existence and the maintenance of balance and security in the region could be considered right intentions for war, since intentions will be considered right when a war is conducted seeking to punish wrongdoers, securing peace and inspiring good (Kruitwagen 2019, 26). Those who wage a war should not do it out of “desire to inflict harm, vengeful cruelty, insatiable animus, savagery in combat, lust for dominance” (Regan 2013, 85).

The main objective of Stuxnet was to cause damage and destroy the centrifuges and it shows a clear level of discrimination because the virus was designed to attack a specific target that was an Iranian nuclear facility and it did not provoke harm to civilians in a direct way. However, some non-combatants’ computers all around the globe have been infected with Stuxnet, but this infection does not pose any harm to their personal safety or the use of their electronic devices because the virus had also an expiration date when it would stop functioning (Schenier 2010) and those infected systems did not match with the target profile (Richardson 2011, 25) that was Iran’s nuclear facilities. The principle of discrimination refers to the mandatory differentiation between soldiers and civilians and to refrain from having an extravagant number of civilian casualties. The civilian casualties should always be unintended, but some can be predicted or expected as a result from an attack on a legitimate military objective (Slater 2012, 52). Non-combatants should not be direct targets of an attack, since they do not pose a military threat, but they are sometimes considered collateral damage while attacking military targets (Lin, Allhoff & Rowe 2012, 25). In some cases, the collateral damage is ethically justifiable in the case that the military objective is considered of high importance and that the unplanned evil inflicted on civilians is low (Slater 2012, 66). In this sense, a case that shows a clear violation of the discrimination principle is the Operation Cast Lead from 2008, an air and heavy artillery attack on extremely populated areas launched by Israel against

Palestine as a response to Hamas terrorist attacks (Slater 2012, 54-55). The Goldstone Commission circulated a report that indicated that at least 1300-1450 Palestianians were killed during the attacks, being the majority of them civilians. Moreover, an Israeli officer publicly said that "When we suspect that a fighter is hiding in a house, we shoot it with a missile and then with two tank shells, and then a bulldozer hits the wall. It causes damage but it prevents the loss of life among soldiers" (Harel 2009), violating the discrimination principles because a simple conjecture is sufficient to destroy the houses of the civilian population.

Stuxnet could be considered as a last resort attack, due to the fact that several steps were taken before the actual attack: in 2003, the International Atomic Energy Agency (IAEA) adopted a resolution ordering Iran to suspend all uranium enrichment activities, which Iran agrees to meet IAEA's demands and ratified a protocol which would allow IAEA's inspectors to have access to the nuclear sites. However, in 2004, Iran refuses to cooperate with IAEA and in 2005 the IAEA issues a new resolution stating that Iran is non-compliant and refers Iran to the UN Security Council. As a consequence, the UN Security Council adopts Resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010), which require Iran to stop its uranium enrichment and establishes different sanctions to Iran. Iran did not stop its production and did not comply with the UN Security Council Resolutions, therefore it can be stated that all preventive available measures were exhausted before executing Stuxnet. The last resort principle implies that all alternative measures should have been exhausted before resorting to war. In the case of Israel versus Palestine, all alternative measures were not exhausted since Israel refused to negotiate with Hamas and ignored the last one's cease-fire propositions (Slater 2012, 58). Moreover, in 2006, a year later after the Israeli withdrawal of Gaza, the newly elected Hamas Congressmen sent a message to Israel saying that it "would pledge not to carry out any violent actions against Israel and would even prevent other Palestinian organizations from doing do" (Ravid 2008). However, Israel continued with attacks that killed at least 660 Palestinian civilians, and continued to escalate the conflict in the following years, despite the fact that a truce was negotiated in 2008 (Khoury 2008), meaning that the last resort principles was not taken into consideration as such, resulting in an unjust attack from Israel.

In conclusion, Classical JWT offers an adequate moral guidance in state sponsored cyber-attacks: under the light of JWT Stuxnet is an unjust cyber-attack against Iran's nuclear programme because the attackers did not follow the JWT principles as a whole and there was no restraint to war. It was allegedly executed by the United States and Israel, which means that still no state claimed its authorship and, as a consequence, Iran would not be able to retaliate because it is not morally permissible to counter-attack without knowing the attacker's identity. However, there are several indications that it was the United States and Israel who developed the malware and perpetrated the cyber-attack. In this sense, they did not have a just cause to carry out the attack since a preventive attack is not considered as a just cause in the tradition. There were no aggressions from Iran, no destruction of property, and therefore no need to punish a wrongdoing. Regardless of the intentions that the United States and Israel had to delay Iran's nuclear programme, which was seen as a threat to the region and international security, without a just cause a war will always be unjust. From the just cause derive all the other principles, especially right intention and proportionality, which will be measured in relation to the pursuit of the just cause. With the absence of the just cause, a proportional counter-measure cannot be assessed and the right intentions will be absent. The lack of competent authority to declare the need for the attack and to establish what is the just cause that the war will be fought for indicate that the attack meant to delay Iran's nuclear programme for several years without the need of formally declaring a war. These types of actions should be considered immoral and states should use the JWT principles as a guide in order to avoid future unjust cyber-attacks.

State-sponsored cyber-attacks are becoming more frequent, which is why state leaders need a moral guidance in order to limit the resort to armed violence and to inflict as little harm as possible. The following chapter will further discuss the application of Classical JWT principles to two cyber-attacks that occurred within an ongoing international armed conflict: the Russo-Ukrainian war.

Chapter 3: Black Energy and Industroyer-Crashoverride

Referring to the previous discussion of the events of the Stuxnet cyber-attack and the United States and Israel's involvement and behaviour in it, this chapter will assess the Black Energy and Industroyer-Crashoverride cyber-attacks under the light of Classical JWT, which understands that war is an ultimate last resort when all alternative non-violent measures have been exhausted and that seeks to restore a long-lasting peace.

This chapter will depict the main events of the BlackEnergy and Industroyer cyber-attacks, as well as the key developments of the war between Russia and Ukraine, and will examine them under the scope of the *jus ad bellum* and the *jus in bello* principles. Industroyer or Crashoverride is a type of malware that is capable of digital remote control of electricity substations, and their switches and circuit breakers, with the aim of disrupting their normal processes by closing down vital energy systems (Cherepanov & Lipovsky, 2017). Black Energy is a type of malware that is utilized on spear-phishing emails that have malicious Microsoft Excel spreadsheets infected with malware, that when opened, it infects the whole system (Kaspersky Labs 2016). Just as Stuxnet, these cyber-attacks had physical effects in the real world because they affected electric power grids, leaving the civil society with no electricity for several hours (Sebenius 2017), being the first automatic grid attacks and marking a massive intensification in the use and propagation of cyberweapons (Groll 2016). The cyber-attacks to the Ukrainian power grid provoked physical damage and economic losses to Ukraine, within the context of an ongoing military conflict. They were also presumably initiated by Russia as part of a hybrid war what has been waging against Ukraine with the aim of causing chaos and panic across the population. BlackEnergy and Industroyer targeted civilian infrastructure, but that were carried out without a just cause, were not commanded by the competent authority, did not follow the proportionality principle, had impure intentions and did not discriminate between military and non-military objectives. As a consequence, they should be considered unjust in the realm of the JWT because they failed to comply with the jus ad bellum and jus in bello principles. The case studies of Industroyer-Crashoverride are essential for this thesis because they are considered akin to Stuxnet, they allegedly originated from one state, targeted another state and caused actual physical harm over critical infrastructure of civilian population (Knake 2018).

Russia did not have a just cause to perpetrate the cyber-attacks against Ukraine's power grid since there was no actual attack from Ukraine towards Russia's territorial integrity nor towards its Russian citizens that were inhabiting in Crimea, thus no wrongdoing was made. On the contrary, Russia has always considered both Ukraine and Belarus as parts of itself, although they were lost as a consequence of the fall of the Soviet Union (Bercean 2016, 156). Vladimir Putin stated during the 2008 NATO Summit in Bucharest that Ukraine is not a state and that if it was accepted as a NATO member, it would cease to exist (Kommersant 2008, 9). As a consequence of NATO's openness to new member states, Russia felt threatened by the West (Snegovaya 2014, 9-12) and its concern over "regime change and a color revolution" (Reisinger & Golts 2014, 2) made Putin utilize every convenient and possible instrument or mechanism to impede NATO's expansion beyond its current limits. On 21 November 2013, the pro-Russian Ukrainian Government decided not to sign an Association Agreement with the European Union, causing the so called Maidan protests that were led by pro-Europe Ukrainian citizens. The protests rapidly escalated due to violent clashes between the police and the agitators, who were against Yanukovych's administration and urged for his resignation. On February 2014, the Ukrainian parliament intended to pass different laws about languages of minorities and to make Ukrainian the official language of the state and other laws that limited the freedom of expression, assembly and association (Pyung-Kyun 2015, 387). As a result, violent demonstrations were held over the following weeks, and the Russian authorities wanted protect the ethnic Russians and the Russian speakers in Crimea from alleged persecution and discrimination (Pyung-Kyun 2015, 387), despite the fact that there were no actual cases of threats or persecution (Galiev 2014). The Russian administration started their propaganda of protecting ethnic Russians while strongly criticizing the Ukrainian national movement. Russia passed laws that stated its compromise to protect Russian compatriots outside of its territorial limits (Coalson 2014) and, consequently, President Vladimir Putin military invaded and annexed Crimea to the Russian Federation's territory on 18 March 2014, after the voting of a referendum which resulted in the biggest political and military crisis in the Eurasian region since the fall of the Soviet Union (Pyung-Kyun 2015**,** 386 and Freedman 2014, 12-13). The United Nations declared the referendum invalid and called the international community to "not recognize any alteration of the status of the Autonomous Republic of Crimea" (United Nations Resolution 2014).

Since the annexation of Crimea, Russia has been having a never ending proxy war in Eastern Ukraine (Paul 2015, 41): the Russian government has also targeted through cyberattacks several Ukrainian institutions causing massive economic losses and the destruction and deterioration of digital and crucial infrastructure (Pernik 2018, 63). In this sense, Russia migrated the conflict from military ground fighting to destructive cyber-activities in order to provoke harm in Ukraine's critical infrastructure, especially in the electricity, energy and economic sectors (Pernik 2018, 63-64). In the last months of 2016 only, Ukrainian public institutions were hit by more than 6500 Russian hack attack that intended to sabotage the critical infrastructure facilities of the country (Zinets 2016). As a consequence to the military action between both countries, the International Criminal Court (ICC), on its 2016 Report on Preliminary Examination Activities, stated that according to the information available it can be concluded that the current affairs in the territory of Crimea "amounts to an international armed conflict between Ukraine and the Russian Federation" and that it started at least when Russian armed forces were sent to the Ukrainian territory without explicit consent of the Ukrainian government (ICC Report 2016, 35).

Ukaine, on the other hand, has a just cause to respond to Russia's invasion and illegal annexation of Ukraine's sovereign territory and to the two cyber-attacks to Ukraine's power grid. The latter were utilized as a means of force to disturb Ukraine's physical and critical infrastructure to get a political advantage (Lindsay 2013, 372) by disrupting the civil population's access to electricity. Following the Just

War Tradition, there are three just causes to morally justify a war: the destruction of property, the right to defend oneself and the right to vindicate suffering and penalize a wrongdoing (Cicero 1991, 11-13). Ukraine would have a just cause to retaliate and counter-attack Russia because it would fulfil the three causes to justify a war: it suffered the destruction of its power grid systems, it has the right to defend its territorial integrity from illegal annexations and to penalize a wrongdoing in the hands of Russia. However, the Russian administration has been completely unsuccessful to adequately justify a just cause for attacking the power grid, as well as a just cause to military intervene and violate Ukraine’s territorial integrity and political sovereignty (Fischer 2016).

The attribution problem arises in the BlackEnergy and Industroyer cyber-attacks due to the velocity and anonymity of the attackers (Shackelford & Andres 2011, 971), making it difficult to prove the responsibility of a certain state and to differentiate the conduct of terrorists, lawbreakers and states themselves (White House 2003, viii). This is a recurring problem that arises in cyberspace, because states can accept that cyber-attacks originate from their territory but that they did not order nor start them (Dipert 2010). The concept of attribution implies the process of identification of the originators of the attack, since one of the requirements to respond to an attack is to justify a conclusive and plausible identification of the attackers (Herpig and Reinhold 2018, 33) because it would be unjust to attack an innocent party, who would in turn have a just cause to respond. In this sense, cyberattacks have become increasingly challenging to attribute with a high level of certainty, and Russia has denied all accusations based on the fact that there is not enough evidence to back their allegations (Pernik 2018, 53-54).

There is no official document available that proves that the cyber-attacks were ordered by the Kremlin (Shehod 2016, 8), therefore they should be considered unjust because they fail to comply with the competent authority principle. Despite the fact that there was a clear illegal action from Russia towards the territorial integrity of Ukraine and that the two cyber-attacks were aimed to critical civilian infrastructure with the aims of causing chaos, there are no reports that reflect a governmental decision to pursue cyber-attacks. Moreover, the Kremlin spokesman Dmitry Peskov stated that ‘there is no war between Ukraine and Russia’ and that Ukraine was suffering from a civil war that ended with Crimea being annexed to Russia in order to protect its Russian ethnics and Russian speaking population (The Moscow Times, 2019). However, taking into consideration the context of the Russo-Ukrainian war, the resources and time invested in the development of the code, the in-depth analysis of the infrastructure of the power grid and the different stages of the cyber-aggression it can be expressed that it was a state-sponsored cyber-attack that was perpetrated by Russia (Polityuk 2017). Russia has been sending troops and military supplies to Crimea and has been waging a ‘hybrid war’ against Ukraine, meaning that it has been attacking financial institutions, the transport system and electric facilities in order to cause panic among the population Polityuk 2017).

Within the context of the Russian-Ukrainian war, Russia’s intentions are impure because it was looking for a territorial expansion when it annexed Crimea after a referendum that was considered illegal by the international community. Moreover, BlackEnergy and Industroyer have been part of a bigger dimension of warfare that had the aim of pursuing the territorial expansion of the Russian Federation. Russia has been expanding its territory into other foreign states such as South Ossetia and Transnistria, regions of Georgia and Moldova (Karnitshing 2014 and Wolff 2015). Russia has also been targeting Russian-speaking citizens from former Soviet Union republics, influencing them with propaganda against the West, occupying territories such as Georgia, Moldova and Ukraine and imposing economic sanctions on them, and has stationed soldiers, with the acceptance of the host states, in Armenia and Belarus (Bond 2017, 1-2). The right intention principle is a subjective criterion that concerns the real intentions of the ones responsible for declaring war in order to eliminate egoistical or hidden motivations for officially declaring war. This means that right intention takes place in an armed conflict when a belligerent’s objectives in resorting to war are the punishment of a wrongdoing and the restoration of peace (Swift 1983, 127). Observing the actions of those involved in a war will aid identify if the principle is satisfied or not so that wrong intentions like violence, revenge or lust for power can be discarded. This principle is connected to just cause because right intention understands that war should only be fought for a just cause thus limiting war objectives to defending that just cause (Regan 2013, 85-86). In this sense, the right intention criterion excludes situations such as territorial growth and pure economic advantages and it implies the intention to amend or remedy the wrong described in the just cause (Fisher 2011, 72), so since Russia did not have a just cause to attack Ukraine's power grid and illegally annexed part of its territory, it can be rightfully stated that there its intentions to pursue the cyber-attacks were impure.

Russia also fails to comply with the proportionality principle because, although the results of the cyber-attacks can be measured and quantified, there is no just cause to measure the amount of harm that should have been inflicted on Ukraine. The cyber-attacks provoked physical harm to the power grid, caused economic losses to the company and to its clients and left part of the population with no electricity or heat for several hours during a cold day in the winter. In this sense, proportionality implies the consideration of the badness that will result from going to war, and balancing it with the good that will arise of the damages that will be avoided (Brown 2003). It is also a principle that is present in both *jus ad bellum* and *jus in bello*: there should be a balanced and comparable reaction and it should be limited and proportionate to the aims of the war and the circumstances that comprise the just cause (US Catholic Bishops 1992, 98-102). Thus, proportionality is inherently connected to both the just cause and discrimination principles. Its relation with the first one has to do with the fact that the good that a state wants to accomplish should be associated with the just cause because a political leader is not free to determine which goods he appreciates or wants (Fisher 2011, 75). On the other hand, proportionality and discrimination limit the acts of those individuals that are immersed in military actions (Royden 2014, 117): the amount of harm inflicted should be commensurate to that received and it should distinguish between military and civilians.

The cyber-attacks did not discriminate between military and non-military targets, therefore they did not respect the discrimination principle. The malware attacked a power-grid that provided electricity to the civilian population and it was part of the civil infrastructure, therefore not connected with the military and attacking it did not offer a military advantage. Moreover, the harm made to the grid and the Ukrainian population should not be considered ‘collateral damage’ because the attack did not suppose a benefit or favored position for Russia. The discrimination principle involves making a differentiation between civilians and soldiers with the aim of avoiding an exorbitant number of civilian fatalities that are unintentional but may be expected from an attack to a military target (Slater 2012, 52). This also means that attacks should be limited to military targets that would offer a categorical military advantage, and those that are not considered military objectives are recognized as civilian objects (AP I 1977, arts. 52.1 and 52.2). In order to identify a military target and differentiate it from a civilian object, an analysis has to be made on its use and objectives. This means that if a power grid is utilized to provide energy to a military facility, then the power grid should be considered a military target.

The fact that the attackers performed two cyber-attacks within a year that targeted the same type of infrastructure reinforces the idea that they had a deep understanding of the internal system of the power grid, therefore they would have a high chance of succeeding in their aims. On December 2015, the first cyber-attack took place by infiltrating the distribution control centers of electricity through the use of software vulnerabilities, hijacking credentials and utilizing a complex and advanced malware. This cyber-attack was initiated by a type of BlackEnergy malware that accessed the power grid network due to the fact that an employee of the Prykarpattya Oblenergo opened an email that contained an infected Excel spreadsheet. This type of attack intended to perform a reconnaissance of the power grid systems and later carry out a disruptive attack. In order to collect all the necessary data to pursue the attack, the malware was remotely controlled by hackers in order to expose different vulnerabilities in the power grid (Bock 2017). These elements allowed the attackers to expose the circuit breakers of three energy distribution companies and to shut down electricity power to over 250.000 citizens during December 2015 (E-ISAC 2016, 1). The second cyber-attack was carried out by using a different type of malware, called Industroyer or Crashoverride that was specifically designed to cause power outages. The attack was fully automated and the attackers could access the power-grid's systems and execute commands to modify the flow of electrical energy. In this sense, the attackers had clearly established a plan with different stages that aimed to cause a massive electricity blackout, and due to the low security systems of the power grid, they had a high chance of succeeding in their objectives.

Before the Black Energy and Industroyer cyber-attacks, no real alternative measures were taken to avoid the resort to war between Russia and Ukraine: no diplomatic communications were made, which precipitated the armed conflict. Two weeks before the annexation of Crimea, Russia sent unmarked uniformed troops to Ukraine in order to support pro-Russian deputies, who chose a new prime minister and demanded the need for a referendum to establish the future status of Crimea (Gregory 2016). Last resort implies taking into consideration the pain and devastation caused by war, and the resort to war should be made only when other alternatives have been unsuccessful or ineffective (Brown 2011). In this case, war has not been the last resort, failing to accomplish the main objective of just war which is to avoid war at all costs and only resorting to war when there are no other options.

In conclusion, under the light of Classical JWT, the BlackEnergy and Industroyer cyberattacks are considered morally unjust because they fail to comply with the just cause, competent authority, right intentions, proportionality, discrimination and last resort criteria. These cyber-attacks present a similar issue as Stuxnet: although it proves to be difficult to assess the identity of the attackers, there are certain indications that it was Russia who perpetrated the attack in order to cause chaos and disorder within the Ukrainian society. Russia did not have a just cause to detriment Ukraine's territorial sovereignty by annexing Crimea and it certainly did not prove to have the right intentions in doing so. In relation to the cyber-attacks, although the ICC stated that there was an on-going military conflict between the two countries, there was no military advantage in attacking the power grid because it was part of the civilian infrastructure and not a military objective. Moreover, in the absence of a just cause, the proportionality principle could not be followed as there was no way to measure the punishment of a wrongdoing. Besides, Russia had impure intentions, it had no just cause to attack the power grid since it received no harm from Ukraine, it deliberately attacked a non-military object, there was no official declaration of war by the competent authority and war was not the last resort, therefore the cyber-attacks are considered unjust under the scope of JWT.

Conclusion

In the bosom of the ongoing technological transformations, the development of new technologies and the increase of cyber-activity, Classical JWT prevails as the leading theory to address the examination of the ethics of war and offers a clear framework that seeks to limit the resort to war. In this essay I argue that Classical JWT is able to address modern issues related to war and can adapt to current moral questions because the means and weaponry used have changed but not the nature of war itself. In this sense, guns and tanks have been interchanged to viruses and malware that attack physical infrastructure and aim to achieve a political advantage over the adversary. By developing ethics into the evolution and utilization of cyberweapons, it can be guaranteed that war is no more atrocious and brutal than it already is (Lin, Allhoff & Rowe 2012).

It was the main objective of this thesis to understand how Classical JWT could offer a moral guidance in state-sponsored cyber-attacks. In doing so, it developed the different criteria that aim to limit the resort to war and to avoid unnecessary harm and destruction, and utilized two main case studies in order to explore the ways that JWT offers guidance for states and politicians.

In chapter one, it was stated that JWT should be understood as a restraint to war and a limitation of destructiveness, with the aims of restoring peace and justice and to punish wrongdoing, and not as a legitimization of the use of force (Rengger 2002, 354-356 and Rengger 2013, 65). The criteria for JWT, *jus ad bellum* and *jus in bello*, have been set and it has been argued that they should not be interpreted as a mere checklist to declare war, but as a guide to use war as a last resort and to look for better non-violent alternatives. If any of the principles are not followed when resorting to war, then that particular war can never be considered just. An essential and arising issue related to the applicability of the JWT principles is that of attribution: the identification of the attacker should be known so as to answer in a just way. This means that the counter-response should target the appropriate attacker in order to avoid wrongfully causing harm to erroneous individuals for an act they did not carry out (Dipert 2010, 401). Moreover, the main and most important principle is that of just cause, due to the fact that all other principles are related to it. Without a just cause, there would be no moral justification for resorting to armed force, because the just cause directs the ends for which waging a war would be justified. The principles of competent authority, proportionality, right intention and reasonable hope of success depend on the just cause and should be measured in relation to it.

In chapter, two the Stuxnet case was studied under the scope of JWT and it was stated that it was a morally unjust cyber-attack against Iran due to the fact that the aggressors did not comply with all of the JWT principles. At the time of the cyber-attack, no just cause existed that could validate the resort to force. Moreover, since the attack was anonymous and was allegedly planned and perpetrated by the United States and Israel, the cyber-attack fails to comply with the competent authority, proportionality and right intention principles. The attribution of the attack is fundamental because self-defense and the punishment of wrongdoing should be aimed to the right aggressor, implying that if there is no knowledge of the authorship then a proportional counter-attack based on the premise of self-defense could not be pursuit. Although there are certain indications that Israel and the United States were behind Stuxnet, no official confirmation has been issued, thus the competent authority and right intention principles are not present. Without the competent authority declaring war, any military action could be considered a terrorist act or banditry and the subjective right intentions for resorting to war cannot be assessed.

In chapter three, two cyber-attacks within the context of the Russo-Ukrainian war were considered under the light of JWT. The two cyber-attacks aimed to destroy civilian infrastructure and the attackers did not have a just cause to do so, therefore they should be considered unjust in the realm of morality. Due to the anonymity of the attacks, it is difficult to assess the identity of the perpetrators and thus, the competent authority principle was not followed, despite the fact that but there are indications that it was Russia who was behind them. In this sense, Russia did not have a just cause to attack Ukraine's infrastructure, and since it was civilian infrastructure that was at stake, the attacks did not comply with the discrimination principle. Moreover, due to the absence of a just cause, the principle of proportionality could not be complied with. Since Russia allegedly attacked non-military targets without and official declaration of war from a competent authority without completing previous diplomatic measures to have war as a last resort, the two cyber-attacks are unjust according to the JWT.

In conclusion, Classical JWT does offer a substantive and coherent guidance for states to limit the resort to war and it addresses in a positive way the Stuxnet and BlackEnergy and Industroyer cyberattacks. The theory offers a valuable insight on the problems that current armed conflicts and the development of new technologies pose to states and to the international community. In regards to the attribution problem, states should invest time and resources in developing new technologies that will allow to get a certain way of establishing the authorship of anonymous cyber-attacks. Finally, the imperative peace-making concept that Classical JWT defends should be the basis for every state leader and policy maker because it limits the resort to war, establishing the importance of going through other non-violent alternatives first. This is a crucial topic because the restoration justice, the punishment of a wrongdoing and the pursuit of peace are the objectives that states should have in mind when facing a conflict.

Bibliography

Aloyo, E. (2015), *Just War and the Last of Last Resort*, Ethics and International Affairs, 9:2, pp. 187-201.

AP I (1977), Additional Protocol to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), of June 1977.

Aquinas, T. (1964), *Summa Theologica*, Edited by Thomas Gilby, Timothy McDermott and Edmund Hill, New York: McGraw-Hill.

Aquinas, T. (2012), *Summa Theologica IIa IIae q 40 On War: Aquinas Political Writings*, Edited and translated by R.W. Dyson, Cambridge University Press.

Augustine (1887), *A Select Library of the Nicene and Post-Nicene Fathers of the Christian Church: St. Augustin: The Writings against the Manichæans, and Against the Donatists*. Vol. 4. Edited by Philip Schaff. New York: Christian Literature Company

Augustine (1983), *Questions on the Heptateuch*, 6.10, in Louis J., *The Early Fathers on War and Military Service*, Wilmington: Michael Glazier, Inc.

Augustine (1998), *The City of God Against the Pagans*, R. W. Dyson, trans. (New York: Cambridge University Press, 1998), p. 929.

Augustine (2006), *Questions on the Heptateuch*, in Reichberg, G., Syse, H. and Begby, E. (eds), Ethics of war: Classic and Contemporary Readings, Oxford et all: Blackwell Publishing.

Babaei, A.R. (2008), *Israel's concerns and Iran's Nuclear Programme*, Economic and Political Journal, Volume 43, Issue 6, February 2008.

Bahgat, G. (2006), *Proliferation: The Islamic Republic of Iran*, Iranian Studies, Volume 39, No. 3, September 2006, 307-327.

Bailey, S.D. (1972), *Prohibitions and Restraints in War,* London: Oxford University Press for the Royal Institute of International Affairs, 1972.

Baker, D.P (2011), *To Whom does a Private Military Commander Owe Allegiance?* In (eds) Wolfendale, J. and Tripodi, P., *New Wars and New Soldiers: Military Ethics in the Contemporary World*, Military Defense Ethics Series, Ashgate Publishing Company.

Barry, C. (2011), *A challenge to the reigning theory of the just war*, International Affairs 87:2, 457-466, Blackwell Publishing.

Beaumont, P. (2010), *Stuxnet worm heralds new era of global cyberwar*, The Guardian, September 30, 2010. https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar

Bellamy, A. (2006), *Just Wars: from Cicero to Iraq*, Cambridge, United Kingdom: Cambridge Policy Press.

Bercean, I.N. (2016), *Ukraine: Russia's New Art of War*, Issue No. 21/2016, pp. 155-174.

Bock, P. (2017), *Ukrainian power grids cyberattack: A forensic analysis based on ISA/IEC 62443*, InTech Magazine, March-April 2017, The International Society of Automation.

Boer, T.A. (2008), *With Michael Walzer towards a Just Peace*, in: Anne Marie Reijnen and Peter Tomson, *Europe between Wars: Bonhoeffer, the Struggle for Peace, and the Cultural Heritage. A Salute to Jurjen Wiersma*, Analecta Bruxellensia 13, 2008.

Bond, I. (2017), *Contested space, Eastern Europe between Russia and the EU*, Centre for European Reform, March 2017.

Bose, D. (2018), *Cyber War on Energy Grids and Infrastructure: Implications of the Russia-US Case*, Centre for Land Warfare Studies (CLAWS) Journal, Summer 2018, New Delhi, India.

Bowen, W. Q. & Kid, J. (2004), *The Iranian Nuclear Challenge*, Journal of International Affairs, Volume 80, Issue 2, pp. 257-67.

Boyle, J. (1996), *Just War Thinking in Natural Law*, in The Ethics of War and Peace: Religious and Secular Perspectives, ed. Terry Nardin, Princeton: Princeton University Press.

Bull, H. (1979), *Recapturing the Just War for Political Theory*, in World Politics, 31(4), July 1979, pp. 588-599.

Burkhardt, T. (2017), *Just War and Human Rights: Fighting with Right Intention*, State University Press of New York Press, Albany.

Burton, J. (2015), *NATO's cyber defence: Strategic challenges and institutional adaptation*, Defence Studies, Volume 15, Issue 4.

Braun, C.N. (2018), *Just War and the Question of Authority,* Zeitschrift fur Ethik und Moralphilosophie, Volume 1, Issue No. 2, pp. 221-236.

Brown, G.D. (2003), *Proportionality and Just War*, Journal of Military Ethics, Volume 2, Number 3, pp. 171-185.

Brown, D. (2011), *Introduction: The Just War Tradition and the Continuing Challenges to World Public Order*, Journal of Military Ethics, 10:3, September 2011, pp. 125-32.

Bruce, I. (2006), *Israelis Plan Pre-emptive Strike on Iran*, Herald, London, January 10, 2006.

Carr, J. (2011), *Inside Cyber Warfare: Mapping the Cyber Underworld*, O'Reilly Media, 2nd Edition, December 2011.

Carr, C.L. and Kinsella, D.T (2013), *Preemption, Prevention and Just ad Bellum*, Political Science Faculty Publications and Presentations, 17, Portland State University.

Carmola, K. (2005), *The Concept of proportionality: Old questions and New Ambiguities*, in Evans, Mark (Ed), *Just War Theory: A reappraisal*, New York: Palgrave McMillan.

Cherepanov, A and Lipovsky, R. (2017), *Industroyer: Biggest threat to industrial control systems since Stuxnet*, We Live Security by ESET, June 12, 2017.

Childress, J.F. (1980), *Just war criteria*, in Shannon, T.A. (Ed), *War or Peace? The Search for New Answers*, Maryknoll, N.Y., Orbis.

Childress, J. (1986), *Just War Theories: The bases, interrelations, priorities and functions of their criteria* in Wakin M.M (ed), *War, Morality and the Military Profession*, second edition, Westview Press, Bouldera Colorado, pp. 256-76.

Cicero (1991), *On Duties*, edited by E.M. Atkins and M.T. Griffin, Cambridge: Cambridge University Press.

Cherepanov, A. and Lipovsky, R. (2016), *BlackEnergy - what we really know about the notorious cyber-attacks*, Virus Bulletin October 2016, ESET, Slovakia.

Childress, (1986), *Just War Theories: The Bases, Interrelations, Priorities, and Functions of Their Criteria* in Malham M. Wakin (ed), *War, Morality, and the Military Profession*, 2nd edition, Westview Press: Boulder.

Chubin, S. (2007), *Iran's Nuclear Ambitions*, Carnegie Endowment for International Peace, Washington DC.

CNSS Committee on National Security Systems (2010), CNSS Instruction No. 4006, 26 April 2010. https://www.hsdl.org/?abstract&did=7447

Coady, C.A.J. (2008), *Morality and Political Violence*, Mises Review 14, No. 1, Spring 2008, Cambridge University Press.

Coalson, R (2014), *Putin Pledges to protect all ethnic Russians anywhere. So, Where are they?*, Radio Free Europe, April 10, 2014.

Coates, A.J. (2016), *The Ethics of War*, Manchester: Manchester University Press.

Cole, D. (2011), *War and intention*, Journal of Military Ethics, Volume 10, Issue 3, pp. 174-191.

Coleman, S. (2013), *Military Ethics: An Introduction with Case Studies*, Oxford: Oxford University Press.

Cook, J. (2010), *Cyberation and Just War Doctrine: A response to Randall Dipert*, Journal of Military Ethics, Volume 9, Issue 4, pp. 411-423.

Cox, R. (2014), *The Ethics of War up to Thomas Aquinas*, in Lazar, S. and Frowe, H. (eds) *The Oxford Handbookd of Ethics of War*, Oxford University Press.

Crawford, N.C. (2003), *Just War Theory and the U.S. Counterterror War,* American Political Science Association, March 2003, Volume 1, Issue No. 1.

Daryl Charles, J. & Corey, D.D. (2012), *The Just War Tradition: An Introduction (American Ideals and Institutions)*, Intercollegiate Studies Institute, 1st edition.

De Vitoria, F. (1991) *Political Writings*, ed., Anthony Pagden, trans., Jeremy Lawrance, Cambridge: Cambridge University Press.

De Vitoria (2001), *On the Law of War*, in Anthony Padgen & Jeremy Lawrance (eds), Francisco de Vitoria: Political Writings, Cambridge University Press.

Dipert, R. (2010), *The Ethics of Cyberwarfare*, Journal of Military Ethics, Volume 9, Issue 4, Special Issue: Ethics and Emerging Military Technologies.

Dueck, C. and Takeyh, R. (2007), *Iran's Nuclear Challenge*, Political Science Quarterly 122, no. 2, Summer 2007.

Durante, M. (2015) *Violence, just cyber war and information*, Philosophy and Technology, Volume 28, pp. 369–385.

Eberle, C. J. (2013), *Just War and Cyberwar*, Journal of Military Ethics, Volume 12, No. 1, pp. 54-67.

Eckert, A (2014), *Private Military Companies and the Reasonable Chance of Success*, in Gentry, C.E. The Future of Just War: New Critical Essays, Studies in Security and International Affairs, University of Georgia Press.

E-ISAC, Electricity Information Sharing and Analysis Center (2016), *Analysis of the Cyber Attack on the Ukranian Power Grid, Defense Use Case*, Industrial Control Systems, March 18, 2016.

Elshtain, J.B. (2003), *Just War against Terror: The Burden of American Power in a Violent World*, Basic Books, Perseus Books Group, New York.

European Commission (2018), *State of the Union 2018 - Cybersecurity: Commission proposes to invest in stronger and pioneering cybersecurity capacity in the EU*, Digital Single Market, 12 September 2018. https://ec.europa.eu/digital-single-market/en/news/state-union-2018-cybersecurity-commission-proposes-invest-stronger-and-pioneering-cybersecurity

Evans, M. (2005), *Just War Theory: A reappraisal*, Edinburgh: Edinburgh University Press.

Fabre, C. (2008), *Cosmopolitanism, Just War Theory and legitimate authority*, International Affairs, Volume 84, Number 5, pp. 963-976.

Falliere, N., Murchu, L.O and Chien, E. (2011), *W32, Stuxnet Dossier*, Symantec Security Response, version 1.4, February 2011.

Farwell, J.P. and Rohozinski, R. (2011), *Stuxnet and the Future of Cyberwar*, Survival, Volume 53, No. 1, pp. 23-40.

Federman, J. (2006), *Israel Hints at Preparation to Stop Iran*, Washington Post, January 22, 2006.

Feiler, T. (2015), *From Dialects to Theo-Logic: The Ethics of War from Paul Ramsey to Oliver O'Donovan*, Studies in Christian Ethics, Vol. 28(3).

Fiala, A. (2008), *The Just War Myth & the Moral Illusions of War*, Lanham: Rowman & Littlefield Publishers, Inc.

Fidler, D. P. (2011), *Was Stuxnet an Act of War? Decoding a Cyberattack*, IEEE Security and Privacy, July-August 2011, pp. 56-59, Vol. 9, Indiana University.

Finkle, Jim (2016), *Hackers used malware to confuse utility in Ukraine outage - report*, Reuters, January 10, 2016. https://www.reuters.com/article/ukraine-cybersecurity-attack/hackers-used-malware-to-confuse-utility-in-ukraine-outage-report-idUKL2N14U01H20160110

Finlay, C.J. (2012), *Fairness and Liability in the Just War: Combatants, Non-combatants and Lawful Irregulars*, Political Studies, March 2013, Volume 61, Issue 1, pp. 142-160.

Finlay, C.J, Parry, J., and Wrange P., (2017), *Introduction: Legitimate Authority, War and the Ethics of Rebellion*, Ethics and International Affairs, Sum, Volume 31, Number 2, pp. 167-168.

Finlay, C.J. (2018) *Just War, Cyber War and the Concept of Violence*, Christopher J. Finlay, Philosophy and Technology, 2018, Vol. 31 (3), pp. 357-377.

Fisher, D (2011), *Morality and War: Can War be Just in the Twenty-First Century?*, Oxford: Oxford University Press.

Fischer, S. (2016), *The Unresolved Conflicts over Transnistria, Abkhazia, South Ossetia and Nagorno-Karabakh in Light of the Crisis over Ukraine*, SWP Research Paper, Stiftung Wissenschaft und Politik German Institute for International and Security Affairs, Berlin, September 2016.

Fitzsimmons, S. (2015), *Just War Theory and Private Security Companies*, International Affairs, 91:5, The Royal Institute of International Affairs, John Wiley and Sons Ltd.

Fotion, N. (2007), *War & Ethics: A new just war theory*, London, Continuum International Publishing Group.

Forge, J. (2009), *Proportionality, Just War Theory and Weapons Innovation*, Science and Engineering Ethics, March 2009, Volume 15, Issue 1, pp. 25-38.

French, S.E. (2018), *Distinction and Civilian Immunity* in Larry Mat, ed, *The Cambridge Handbook of the Just War*, Cambridge University Press.

Frowe, H. (2011), *The Ethics of War and Peace: An Introduction*, Abingdon, Routledge.

Galiev, A (2014), *Putin's Game of Shadows: Hybrid War in Ukraine, Propaganda and Fascism*, Amazon Digital Service, Inc.

Gasiorowski, M. (2007), *The New Aggressiveness in Iran's Foreign Policy*, Journal of Middle East Policy, Volume 14, Issue 2, pp. 126-32.

Gjelten, T. (2010) *Shadow wars: Debating cyber disarmament*, World Affairs, November/December, Volume 173, Issue 4, pp. 33–42.

Gray, C.S. (2007), *The Implications of Preemptive and Preventive War Doctrines: A Reconsideration*, Army War College, Strategic Studies Institute, U.S. Government.

Gorman, R.R. (2010), *War and the Virtues in Aquinas's Ethical Thought*, Journal of Military Ethics, Volume 9, Issue 3, pp. 245-261.

Goutam, R.K. (2015), *Importance of Cyber Security*, International Journal of Computer Applications, Volume 111, No. 7, February 2015.

Gray, C. S. (2010), *The Strategy Bridge: Theory for Practice,* Oxford: Oxford University Press.

Gregory, P.R. (2016), *International Criminal Court: Russia's Invasion of Ukraine is a 'Crime', not a Civil War*, Forbes, November 20, 2016. https://www.forbes.com/sites/paulroderickgregory/2016/11/20/international-criminal-court-russias-invasion-of-ukraine-is-a-crime-not-a-civil-war/

Groll, E. (2016), *Did Russia knock out Ukraine's Power Grid?,* Foreign Policy, January 8, 2016. https://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/

Groll, E. (2016), *'Obama's General' Pleads Guilty to Leaking Stuxnet Operation*, Foreign Policy, October 17, 2016.

https://foreignpolicy.com/2016/10/17/obamas-general-pleads-guilty-to-leaking-stuxnet-operation/

Grotius in Richard Tuck (2005) *The Rights of war and Peace: In Three Volumes*, Indianapolis, Liberty Fund Incorporated.

Grotius (2013), *On the Rights of War and Peace*, edited by Stephen C. Neff, Cambridge University Press.

Halliday, J. (2010), *Stuxnet worm is the 'work of a national government agency'*, The Guardian, September 24, 2010. https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency

Harbour, F.V. (2011), *Reasonable Probability of Success as a Moral Criterion in the Western Just War Tradition*, Journal of Military Ethics, Volume 10, Number 3, pp. 230-241.

Harel, A. (2009), *IDF Officer: 'It Will Take Many Years to Restore Bomb-Wracked* Gaza', Haaretz, January 7, 2009. https://www.haaretz.com/1.5059381

Hartle, A. (2004), *Moral issues in military decision making*, 2nd ed. Lawrence: University Press of Kansas.

Heinze, E.A. and Steele, B.J. eds. (2009) *Ethics, Authority, and War: Non-State Actors and the Just War Tradition*. New York: Palgrave Macmillan.

Herberg-Rothe, A. & W. Honig (2007), '*War Without End(s): The end of Clausewitz?*', Distinktion, 8(2): 133-150.

Herpig, S. and Reinhold, T. (2018), *Spotting the bear: credible attribution and Russian operations in cyberspace* in Popescu, N. and Secrieru, S. (eds), *Hacks, leaks and disruptions: Russian cyber strategies*, Chaillot Paper N 148, October 2018.

Hudson, K., (2009), *Justice, Intervention and Force in International Relations, Reassessing Just War Theory in the 21st Century*, New York, Rutledge.

Hurka, T. (2005), *Proportionality in the morality of war*, Philosophy & Public Affairs, Vol 33, 34–66.

IISS Strategic Comments (2011), *Stuxnet: targeting Iran's nuclear programme*, Strategic Comments, Volume 17, No. 2, 1-3.

International Criminal Court (ICC) (2016), *Report on Preliminary Examination Activities 2016,* Office of the Prosecutor, 14 November 2016.

Jacobsen, J. T. (2014), *The Cyberwar mirage and the utility of cyberattacks in war: How to make real use of Clausewitz in the age of cyberspace*, Danish Institute for International Studies, 2014:6.

Jenkins, R. (2013), *Is Stuxnet physical? Does it matter?* Journal of Military Ethics, Volume 12, No. 1, 68-79.

Jensen, E.T. (2013), *Cyber Attacks: Proportionality and Precautions in Attack*, International Law Studies 198, Volume 89.

Johnson, J.T. (1981), *Just War Tradition and the Restraint of War: A Moral and Historical Inquiry*, Princeton Legacy Library, Princeton University Press.

Johnson, J.T. (1984), *Can Modern War be Just?,* New Haven: Yale University Press.

Johnson, J. T. (1991), *Just War in the Thought of Paul Ramsey*, Journal of Religious Ethics, Volume 19, No. 2, pp. 183-207.

Johnson, J. T. (1999), *Morality and contemporary warfare*, New Haven: Yale University Press.

Johnson, J.T., (2001), *Authority and Intention*, The Christian Century, November 14, 2001, Vol. 18, No. 31, 27-29.

Johnson, J.T. (2002), *Paul Ramsey and the Recovery of the Just War Idea,* Journal of Military Ethics, Volume 1.

Johnson, J.T. (2003), *Aquinas and Luther on War and Peace: Sovereign Authority and the Use of Armed Force*, Journal of Religious Ethics, Volume 31, Issue 1, February 2003.

Johnson, J.T. (2005), *Just War, as it was and is*, First Things Journal, Institute on Religion and Democracy, January 2005.

Johnson, J.T. (2005), *The War to Oust Saddam Hussein: Just War and the New Face of Conflict*, Lanham, MD: Rowan & Littlefield Publishers Inc.

Johnson, J.T. (2013), *Contemporary Just War Thinking: Which Is Worse, to Have Friends or Critics?*, Ethics & International Affairs, Volume 27, Issue No. 1, pp. 25-45, Carnegie Council for Ethics in International Affairs.

Kapersky Lab (2010), *Kapersky Lab provides its insights on Stuxnet worm*, Corporate News, Kapersky Lab Press Release, September 24, 2010.

Karnitsching, M. (2014), *Russia's Crimea Grab Sparks Wartime Allusions*, Dow Jones &Company Inc, March 7, 2014. https://www.wsj.com/articles/russias-crimea-grab-sparks-wartime-allusions-1394152518

Kaspersky Labs (2016), *BlackEnergy APT attacks in Ukraine*, https://www.kaspersky.com/resource-center/threats/blackenergy

Kerr, P. K. (2015), *Iran's Nuclear Program: Tehran's Compliance with International Obligations*, CRS Report No. R40094, Washington DC: Congressional Research Service.

Khan, R., Maynard, P., McLaughlin, K., Laverty, D., and Sezer, S. (2016), *Threat Analysis of BlackEbergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid*, 4th International Symposium for ICS; SCADA Cyber Security Research, Queen's University Belfast.

Khoury, J. (2008), *Meshal: Shalit Still Alive*, Haaretz, April 1, 2008.

Kim, Y., Kim, I. and Park, N. (2014), *Analysis of Cyber Attacks and Security Intelligence*, Cyber Security Research Laboratory, Electronics and Telecommunications Research Institute, Jeju National University, pp. 489-494.

Knake, R. (2018), *The New Cyber Battleground: Defending the US Power Grid from Russiand Hackers*, Foreign Affairs, July 19, 2018.

Koeman, A. (2007), *A Realistic and Effective Constraint on the Resort to Forc*e, Journal of Military Ethics, Volume 6, No. 3.

Kommersant Newspaper (2008), *NATO bloc sold for blocking*, Online Journal Modelling the New Europe, Interdisciplinary Studies, Issue 57, July 4th, 2008.

Kruitwagen, B. (2019), *Just War or Aggressive Intervention? The Just War Theory and the Saudi-led Intervention in Yemen*, Militaire Spectator, Volume 188, No. 1.

Kunkel, J.C. (1983), *Just War Doctrine and Pacifism*, The Thomist: A Speculative Quarterly Review, The Catholic University of America Press, Volume 47, Number 4, October 1983, pp. 501-512.

Lackey, D. (1982), *A modern theory of Just War*, Ethics, Vol. 92, No. 3, Special Issue: Symposium on Moral Development, University of Chicago Press.

Lackey, D. (1984), *Moral Principles and Nuclear Weapons*, New Jersey, Rowman and Littlefield.

Lackey, Douglas (1989), *The Ethics of War and Peace*, Prentice Hall, Englewood Cliffs, NJ.

Lang, A., O'Driscoll, C., and Williams, J., (2013), *Just War: Authority, Tradition and Practice*, Georgetown University Press.

Langan, J. (1984), *The elements of St. Augustine's Just War Theory*, The Journal of Religious Ethics, Vol. 12, No. 1, Spring 1984, pp. 19-38.

Langan, J. (2001), *The Elements of St. Augustine's Just War Theory*, Journal of Religious Ethics, Vol. 12, Wiley-Blackwell.

Lazar, S. (2016), *War*, Stanford Encyclopedia of Philosophy.

Lebow, N. & Stein, J. (1994). *We all lost the Cold War*. Princeton: Princeton University Press.

Lee, D. (2012), *Flame: Massive cyber-attack discovered, researchers say*, BBC News, May 28, 2012. https://www.bbc.com/news/technology-18238326

Lee, S. (2012), *Ethics and War: An Introduction*, Cambridge Applied Ethics, Cambridge: Cambridge University Press.

Lee, T.H. (2004), *The Augustinian Just War Tradition and the Problem of Pretext in Humanitarian Intervention*, Fordham International Law Journal Volume 28, Issue 3 2004 Article 7, 756-762.

Libicki, M.C (2009), *Cyberdeterrence and Cyberwar*, Project Air Force, RAND Corporation.

Lieberthal, K. and Singer, P. (2012), *Cyber security and US-China Relations*, Washington DC: Brookings Institution.

Liff, A.P. (2012), *Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War*, The Journal of Strategic Studies 35, no. 3 (June 2012).

Lindsay, J.R. (2013), *Stuxnet and the limits of Cyberwarfare*, Security Studies, Volume 22, No. 3, 365-404.

Lin, P., Allhoff, F. and Rowe, N.C. (2012), *Computing Ethics, War 2.0: Cyberweapons and Ethics*, Communications of the ACM, March 2012, Volume 55, No. 3, pp. 24-26.

Lonsdale, D.J. (2004) *The Nature of War in the Information Age: Clausewitzian Future*, New York: MPG Books.

Lucas, G. R. Jr. (2010), *Postmodern War*, Journal of Military Ethics, Volume 9, No. 4, pp. 289-298.

Lynn, W.F. (2010), *Defending a New Domain: The Pentagon's New Cyberstrategy*, Foreign Affairs 89:5 (September/October 2010).

Lynn, W.J.III (2010), *Defending a New Domain: The Pentagon's Cyber Strategy*, Foreign Affairs, September/October 2010, pp. 97-108.

MacAskill, E. and McGreal, C. (2005), *Israel should be wiped off map, says Iran's president*, The Guardian, October 27, 2005. https://www.theguardian.com/world/2005/oct/27/israel.iran

Mahnaimi, U. and Baxter, S. (2005), *Israel Readies Forces for Strike on Nuclear Iran*, Sunday Times, London, December 11, 2005. https://www.thetimes.co.uk/article/israel-readies-forces-for-strike-on-nuclear-iran-063qz38t5dp

McMahan, J. (2006), *Just Cause for War*, Ethics and International Affairs, Volume 19, Issue 3, December 2005, pp. 1-21.

Markoff, J. (2008), *Before the Gunfire, Cyberattacks*, The New York Times, August 12, 2008.

Mattox, J. M. (2018), *The Just War Tradition in Late Antiquity and the Middle Ages*, in May, L. *The Cambridge Handbook of the Just War*, Cambridge: Cambridge University Press.

McKeogh, C. (2002), *Innocent Combatants: the morality of killing in war*, New York, Palgrave Macmillan.

McMahan, J. (1994), *Innocence, Self-defense and Killing in War*, Journal of Political Philosophy, Volume 2, pp. 193-221.

McMahan, J. (2005), *Just Cause for War*, Ethics & International Affairs, Volume 19, Issue 3, Cambridge Council for Ethics in International Affairs, p. 1-21.

McMaster, H. R. (2011), *Moral, Ethical and Psychological Preparation of Soldiers and Units for Combats*, Naval War College Review 64, No. 1 (Winter 2011), 7-19.

Miller, R. (2012), *Aquinas and the Presumption Against Killing in War*, The Journal of Religion, Vol 82, No. 2.

Miller, L. (1964), *The Contemporary Significance of the doctrine of Just* War, World Politics, Vol. 16, No.2, January 1964, Cambridge University Press.

Nakashima, E. and Warrick, J. (2012), *Stuxnet was work of U.S. and Israeli experts, officials say*, The Washington Post, June 2, 2012.

https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?noredirect=on&utm_term=.bdf78b0c815e

NATO North Atlantic Treaty Organization (2019), *NATO Cyber Defence Fact Sheet*, February 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

Neumann, P. (1996), *Security Risks in the Computer-Communication Infrastructure*, adaptation of written testimony from Security in Cyberspace, Hearings, 1996, pp. 350-363.

O'Brien, W.V. (1981), *The Conduct of Just and Limited War*, New York: Editions Praeger.

O'Brien, W.V. (1982), *The Conduct of Just and Limited War*, Greenwood Pub Group.

O'Donovan, O. (2003), *The Just War revisited*, Oxford University Press.

Oliphant, J. (2007), *OCR Religious Ethics for AS and A2,* Routledge Taylor and Francis Group.

Orend, B. (2000), *Michael Walzer on Resorting to Force*, Canadian Journal of Political Science, Vol XXXIII, No 3, p. 535-536.

Orend, B., (2005), *War*, Stanford Encyclopedia of Philosophy.

Orend, B. (2006), *Morality of War*, Ontario: Broadview Press.

Osawa, J. (2017), *The Escalation of State Sponsored Cyber-attack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?* Asia-Pacific Review, 24:2, pp. 113-131.

Parry, J. (2015), *Just War Theory, Legitimate Authority, and Irregular Belligerency*, Philosophia, March 2015, Volume 43, Issue 1.

Parsons, G. (2012), *The Incoherence of Walzer's Just War Theory*, Social Theory and Practice, Vol 38 (4), pp. 663-688.

Parsons, G. (2014)., *What is the Classical Theory of Just Cause? A Response to Reichberg*, Journal Military of Ethics, 12:4, 357-369.

Pattison, J. (2012), *The legitimacy of the military, private military and security companies, and just war theory*, European Journal of Political Theory, II:2.

Pattison, J. (2015), *The ethics of diplomatic criticism: The Responsibility to Protect, Just War Theory and Presumptive Last Resort*, European Journal of International Relations, Volume 21, Issue No. 4, pp. 935-957.

Paul, A. (2015), *The EU in the South Caucasus and the Impact of the Russian-Ukraine War*, The International Spectator, Italian Journal of International Affairs, 50:3, pp. 30-42.

Pernik, P (2018), *The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine*, in Nicu Popescu and Stanislav Secrieru (eds), *Hacks, leaks and disruptions: Russian cyber strategies*, Chaillot Paper N 148, October 2018.

Polityuk, P., Vukmanovic, O., and Jewkes, S. (2017), *Ukraine's power outage was a cyber-attack: Ukrenergo* Technology News, Reuters, January 18, 2017. https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA

Polityuk, P. (2017), *Ukraine points finger at Russian security services in recent cyber-attack*, Cyber Risk, Reuters, July 1st, 2017.https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P

Pyung-Kyung, W. (2015), *The Russian Hybrid War in the Ukraine Crisis: Some Characteristics and Implications*, The Korean Journal of Defense Analysis, Vol. 27, No. 3, September 2015, pp. 383-400.

Ramsey, P. (2002), *The Just War: Force and Political Responsibility*, Rowman and Littlefield Publishers, Inc.

Ramsey, P., and Hallowell, J. H. (2011), *War and the Christian conscience: how shall modern war be conducted justly?*, Duke University Press.

Ravid, B. (2008), *In 2006 Letter to Bush, Haniyeh Offered Compromise with Israel*, Haaretz, November 2008. https://www.haaretz.com/1.5058477

Regan, R.J. (2013), *Just War, Principles and Cases*, Second Edition, The Catholic University of America Press, Washington D.C.

Reichberg, G.M., Syse, H., and Begby, E. (2006), *The ethics of war: classic and contemporary readings*, Oxford, Blackwell Publishing Ltd.

Reichberg, G.M. (2007), *Preventive War in Classical Just War Theory*, Journal of the History of International Law, pp. 5-34.

Reichberg, G.M. (2012), *Legitimate Authority: Aquinas's First Requirement of a Just War*, The Thomist: A speculative Quarterly Review, Volume 76, Number 3, July 2012, pp. 337-369.

Reisinger, H. and Golts, A (2014), *Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence*, NATO Research Paper, Rome: Research Division- NATO Defense College, Volume 105, Issue 11, pp. 1-12.

Reitberger, M. (2013), *License to Kill: Is legitimate authority a requirement for just war?,* International Theory, 5:1, pp. 64-93 Cambridge University Press.

Rengger, N. (2002), *On the Just War Tradition in the Twenty-First Century*, International Affairs, Volume 78, No. 2.

Rengger, N. (2012), *On the Just War Tradition in the Twenty-First Century*, International Affairs (Royal Institute of International Affairs 1944-), Vol. 78, No. 2, April 2002, pp. 353-363.

Rengger, N. (2013), *Just War and International Order, The Uncivil Condition in World Politics*, University of Saint Andrews, Cambridge University Press.

Reuters (2006), *Iran announces it has enriched uranium*, Radio Free Europe Radio Liberty, April 11, 2006. https://www.rferl.org/a/1067592.html

Richardson, J. (2011), *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 John Marshall Journal of Information Technology and Privacy Law, Volume 29, Fall 2011, Article 1.

Ricks, T., (2014), *The Future of war: Cyber is expanding the Clausewitzian spectrum of conflict*, Foreign Policy, November 13, 2014.

Rid, T., (2013) *Cyberwar will not take place*, London: Hurst Publishers.

Rodin, D. (2005) , *War and Self-defense*, Oxford: Oxford University Press.

Royden, A. (2014), *An Alternative to Nuclear Weapons? Proportionality, Discrimination and the Conventional Global Strike Program* in Gentry C.E. and Eckert, A.E. (eds) *The Future of Just War: New Critical Essays*, Athens: University of Georgia Press.

Russell, F. H. (1975), *The Just War in the Middle Ages*, Cambridge: Cambridge University Press.

Sanger, D. E., *Obama order sped up wave of Cyberattacks against Iran*, The New York Times, June 1, 2012. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Schaap, A. J. (2009). *Cyber warfare operations: Development and use under international law*, Air Force Law Review, 64, 121–174.

Schmidt, L., Maratto, S. (2008), *The End of Ethics in a Technological Society*, Queen University Press.

Schneier, B. (2010), *The Story behind the Stuxnet Virus*, Forbes, October 7, 2010. https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#59ad9a4a51e8

Schuurman, B. (2010), 'Clausewitz and the 'New Wars' Scholars', Parameters, Volume 40, Issue 1.

Sebenius, Alyza (2017), *Will Ukraine be hit by yet another Holiday Power-Grid Hack?,* The Atlantic, December 13, 2017. https://www.theatlantic.com/technology/archive/2017/12/ukraine-power-grid-hack/548285/

Shackelford, S.J. & Andres, R.B. (2011), *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, Georgetown Journal of International Law, Summer 2011, Volume 42, Issue 4, pp. 497-1014.

Schulzke, M. (2017), *Just War Theory and Civilian Casualties: Protecting the Victims of War*, Cambridge: Cambridge University Press.

Shehod, A. (2016), *Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US*, Cybersecurity Interdisciplinary Systems Laboratory (CILL), Massachusetts Institute of Technology (MIT).

Singer, P.W. and Friedman, A. (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford: Oxford University Press.

Singer, P.W. (2015), *Stuxnet and its hidden lessons on the ethics of cyberweapons*, 47 Case Western Reserve Journal of International Law 79.

Singer, P.W. and Brooking, E.M. (2018), *What Clausewitz can teach us about war on Social Media: Military Tactics in the Age of Facebook,* Foreign Affairs, October 2018.

Slater, J. (2012), *Just War Moral Philosophy and the 2008-09 Israeli Campaign in Gaza*, International Security, Volume 37, No. 2 (FALL 2012), pp. 44-80, Massachusetts Institute of Technology Press.

Snegovaya, M. (2015), *Putin's Information Warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare*, in Russia Report I, September 2015, pp. 1-28.

Spade, J. M., (2012) *Information as Power: China's Cyber power and America's National Security*, US Army War College.

Suarez, F. (1944), *De Triplici Vitute Theologica, Fide, Spe et Charitate*, [1621], reprinted in Scott, J.S. ed., *Classics of International Law*, Volume 2, Oxford: Clarendon Press.

Swift, L. (1983), *The Early Fathers on War and Military Service*, Wilmington, DE: Michael Glazier.

Symantec (2018), *Internet Security Threat Report 2018*, Symantec Corporation, Volume 23, March 2018.

Symantec (2019), *Internet Security Threat Report 2019*, Symantec Corporation, Volume 24, February 2019.

Syse, H., and Reichberg, G.m. (2007). *Ethics, nationalism and just war: medieval and contemporary perspective*, CUA Press.

Taslaman, C. and Taslaman, F. (2013), *Contemporary Just War Theory: Paul Ramsey and Michael Walzer*, Journal of Academic Studies, November 2013, Vol. 15 (59), pp. 1-20.

Teson, F.R. (2011), *Humanitarian Intervention: Loose Ends*, Journal of Military Ethics 10:3, pp. 192-212.

The Moscow Times (2017), *'There is no War between Ukraine and Russia', Kremlin Claims*, January 30, 2019.

The White House (2002), National Security Strategy of the United States (NSS), September 2002. https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/

The White House (2003), National Strategy to Secure Cyberspace, February 2003. https://www.nitrd.gov/cybersecurity/documents/NationalStrategytoSecureCyberspace2003.pdf

The White House (2019), *Cybersecurity Funding*, Analytical Perspectives, Office of Management and Budget, Chapter 21, pp. 273-287. https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf

Toner, C. (2010). *The logical structure of just war theory*, The Journal of Ethics, 14(2), 81–102.

Traynor, I. (2007), *Russia accused of unleashing cyberwar to disable Estonia*, The Guardian, May 17, 2007.

United Nations (2014), A/RES/68/262, Resolution adopted by the General Assembly on 27 March 2014: Territorial integrity of Ukraine.

US Catholic Bishops (1992), *The Challenge of Peace: God's Promise and Our Response* in Jean Bethke Elshtain, ed., Just War Theory, New York University Press, New York.

USA (2005) *US National Defense Strategy*, http://www.au.af.mil/au/awc/awcgate/nds/nds2005.pdf

Van der Meer, Sico (2018), *State-level responses to massive cyber-attacks: a policy toolbox*, Clingendael, Netherlands Institute of International Relations.

Von Clausewitz, C. (1976), *On War,* edited and translated by Michael Howard and Peter Paret, Princeton, NJ: Princeton University Press.

Von Clausewitz, C. (2007 [1832]), *On War*, translated by M. Howard and P. Paret, edited by B. Heuser, Oxford: Oxford University Press.

Walzer, M., (2015) *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, Basic Books, Perseus Books Group, 5th edition.

Walzer, M., (2004), *Thinking politically, Essays in Political Theory*, New Heaven, Yale University Press.

Walzer, M. (2002), *The argument about Humanitarian Intervention,* Dissent Magazine, Vol. 49, No. 1.

Walzer, M. (2004), *Justice and Injustice in the Gulf War, Arguing about War*, New Heaven, Yale University Press.

Ward, C. (2007), *Israel's Cyber Shot at Syria*, DefenseTech, November 26, 2007. https://www.military.com/defensetech/2007/11/26/israels-cyber-shot-at-syria

Weinberg, S. (2011), *Computer security: Is this the start of cyberwarfare?,* Nature 474, 142-145, 8 June 2011.

Weisman, S. R. (2006), *Cheney Warns of 'Consequences' for Iran on Nuclear Issue*, The New York Times, March 8, 2006.https://www.nytimes.com/2006/03/08/world/cheney-warns-of-consequences-for-iran-on-nuclear-issue.html

Whewell, W. (1853), *Grotius on the rights of war and peace: an abridged translation*, Cambridge University Press.

Wolff, A.T (2015), *The future of NATO enlargement after the Ukraine crisis*, International Affairs, Volume 91, Issue 5, September 2015.

Yoder, J.H. (2001), *When War is Unjust: Being Honest in Just-War Thinking*, Wipf & Stock Publishers, 2nd edition.

Zinets, Natalia (2016), *Ukraine hit by 6500 hack attacks, sees Russian 'cyberwar'*, Reuters World News, December 29, 2016. https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC